Wireless-N 4-Port Router
User's Manual

Copyright 2007 EUSSO Technologies, Inc. All rights reserved.

Contents

BEFORE YOU START IV
Installation Overview iv
PACKING LIST IV
Installation Notes v
Installation Information vi
INTRODUCTION 1
ROUTER DESCRIPTION AND OPERATION 1
FRONT VIEW 2
LED Display 3
REAR PANEL CONNECTIONS 4
CONNECTING DEVICES TO THE ROUTER 5
Connect Router to Ethernet 5
Connecting through 802.11 Wireless 5
General Guide to Setting Up a Wireless Network 5
Installation Considerations for Wireless LAN 7
POWER ON WIRELESS BROADBAND ROUTER 8
Factory Reset Button 8
CONFIGURATION 9
IP SETTINGS ON YOUR COMPUTER 9
ACCESS THE CONFIGURATION MANAGER 9
Login to Home Page 10
WEB MANAGER 11
BASIC CONFIGURATION – HOME DIRECTORY MENUS 12
SETUP WIZARD 13
BASIC WIRELESS SETUP 27
Wireless Security 28
Wi-Fi Protected Setup (WPS) 29
WAN CONFIGURATION 34
Static IP Address Connection 35
Dynamic IP Connection 37
PPPoE Connection 39
Bridge Connection 41
PPTP Connection 42
L2TP Connection 44
LAN 46

DHCP 47
ADVANCED DIRECTORY MENUS 49
Virtual Server 50
Applications 51
Firewall 52
DMZ 53
IP Filters 54
MAC Filters 55
URL Blocking 56
Domain Blocking 57
Wireless Performance 58
Dynamic DNS 59
QoS 60
TOOLS 62
Change System Password 62
Remote Web Access 62
Time 63
SYSTEM 64
Save or Load Configuration File 64
Reset to Factory Default Settings 64
Firmware 65
Miscellaneous 66
STATUS 67
Log 68
Wireless Clients 68
Statistics 68
TECHNICAL SPECIFICATIONS 69
CONFIGURING IP SETTINGS ON YOUR COMPUTER 71

Before You Start

Please read and make sure you understand all the prerequisites for proper installation of your new Wireless Broadband Router. Have all the necessary information and equipment on hand before beginning the installation.

Installation Overview

NOTE: You must have an account setup with an ISP (Internet Service Provider) in order to use this device for Internet access. Contact your preferred broadband Internet service provider to set up an account.

The procedure to install the Wireless Broadband Router can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.
2. Install the hardware, connect the cables to the device and connect the power adapter.
3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based management software built into the Wireless Broadband Router.
4. Use the web-based management software to configure the device to suit the requirements of your Internet service.

Packing List

Open the shipping carton and carefully remove all items. Make sure that you have the items listed here.

- One Wireless-N Broadband Router
- One CD-ROM containing the User's Guide and Quick Installation Guide
- Ethernet cable
- One power adapter suitable for your electric service
- One Quick Installation Guide

CAUTION: The Wireless-N Broadband Router must be used with the power adapter included with the device. Using a power supply with a different voltage rating will damage and void the warranty for this product

If any of the above items are missing, please contact your reseller.

Installation Notes

In order to establish a connection to the Internet it will be necessary to provide information to the router that will be stored in its memory. For some users, only their account information (User Name and Password) is required. For others, various parameters that control and define the Internet connection will be required.

Internet Connection

The Wireless-N Router is intended for use with a broadband device such as an ADSL, xDSL or cable (CATV) modem. The physical connection to the Internet must first be established through a broadband device, typically this should be set up as an invisible bridge.

Operating Systems

The Wireless-N Router uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Microsoft Windows® operating systems.

Web Browser

Any common web browser can be used to configure the router using the web configuration management software. The program is designed to work best with more recently released browsers. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection, firewall software or Internet security packages) that may be running on your computer.

Ethernet or Wireless Adapter

Any computer that uses the router must be able to connect to it through an Ethernet port or through the wireless 802.11n/g/b connection. The computer therefore must have either an Ethernet adapter or 802.11n/g/b adapter installed. Network adapters are standard for most computers sold presently.

Installation Information

Print this page and record the listed information here in case you have to re-configure your WAN (Internet) connection in the future or reset the device configuration settings.

Information you will need from your Internet service provider:		
Username	This is the Username that is used to log on to your Internet service provider's network. It is commonly in the form – user@isp.com.	Record your info here.
Password	This is the Password that is used, in conjunction with the Username above, to log on to your Internet provider's network.	
Internet Connection Type	This is the method that your ISP uses to send and receive data between the Internet and your computer.	
Information you will need about your Wireless-N Router:		
Username	This is the Username you will be prompted to enter when you access the Wireless-N Router configuration screens using a Web browser. The default Username is **admin**.	Record your info here.
Password	This is the Password you will be prompted to enter when you access the Wireless-N Router's configuration windows using a Web browser. The default Password is **admin**.	
LAN IP address	This is the IP address you will enter into the Address field of your Web browser to access the router's configuration windows using a Web Browser. The default IP address is **192.168.1.1**.	
LAN Subnet Mask	This is the subnet mask used by the Wireless-N Router, and will be used throughout your LAN. The default subnet mask is **255.255.255.0**.	
Information you will need about your LAN or computer:		
DHCP Client status	Your Wireless-N Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The range of IP addresses the will assign are from **192.168.1.100** to **192.168.1.199** using the default DHCP server settings. Computers must to be configured to Obtain an IP address automatically (as DHCP clients) to use the DHCP server.	Record your info here.

Information about your Wireless LAN:		
SSID		Record your info here.
Channel		
Authentication		
WEP (Hex/ASCII)	Key 1: Key 2: Key 3: Key 4:	Record your info here.
WPA (802.1x)	RADIUS IP Address: Port: Secret:	
WPA-PSK	Pass phrase:	

Introduction

This section provides a brief description of the router, its associated technologies, and a list of router features.

Router Description and Operation

The Wireless-N Router is designed to provide connectivity for your private Ethernet and 802.11g/802.11b/802.11n wireless network to the Internet via ADSL, xDSL, cable modem or other common broadband connection.

The router is easy to install and use. The four standard Ethernet ports are used to connect computers or other Ethernet devices to the wired LAN (Local Area Network); the embedded wireless access point is used for connecting 802.11b, 802.11g and 802.11n wireless devices.

Router Features

The Wireless-N Router provides the following features:

- **802.11n Wireless LAN** – Wireless connectivity for IEEE 802.11n/802.11g/802.11b workstations and devices.
- **Wi-Fi Protected Status** – Quick, effective and simple wireless security implementation for WPS devices.
- **Broadband Connection Sharing** - Connects multiple computers to a Broadband (Cable or DSL) modem to share the Internet connection.
- **Ethernet Switch -** Allows sharing of an Internet connection with multiple computers and devices.
- **VPN Supported -** Supports multiple and concurrent IPsec and PPTP pass-through sessions, so multiple users behind the Wireless-N Router can access corporate networks through various VPN clients more securely.
- **Advanced Firewall, MAC Filtering, and WebSite Filtering Features -** The Web-based user interface displays a number of advanced network management features including:
- **Port Forwarding Supported -** Enables you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.
- **Special Application Supported -** Special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on. The Wireless-N Router can sense the application type and open a multi-port tunnel for it.
- **DMZ Host Supported -** Allows a networked computer to be fully exposed to the Internet. This function is used when the Special Application feature is insufficient to allow an application to function correctly.

Front View

The LED indicators on the Wireless-N Router are located on the front panel the device.

Front of Wireless Broadband Router

Place the router in a location where it is not exposed to heat and where the LED indicators are visible.

LED Display

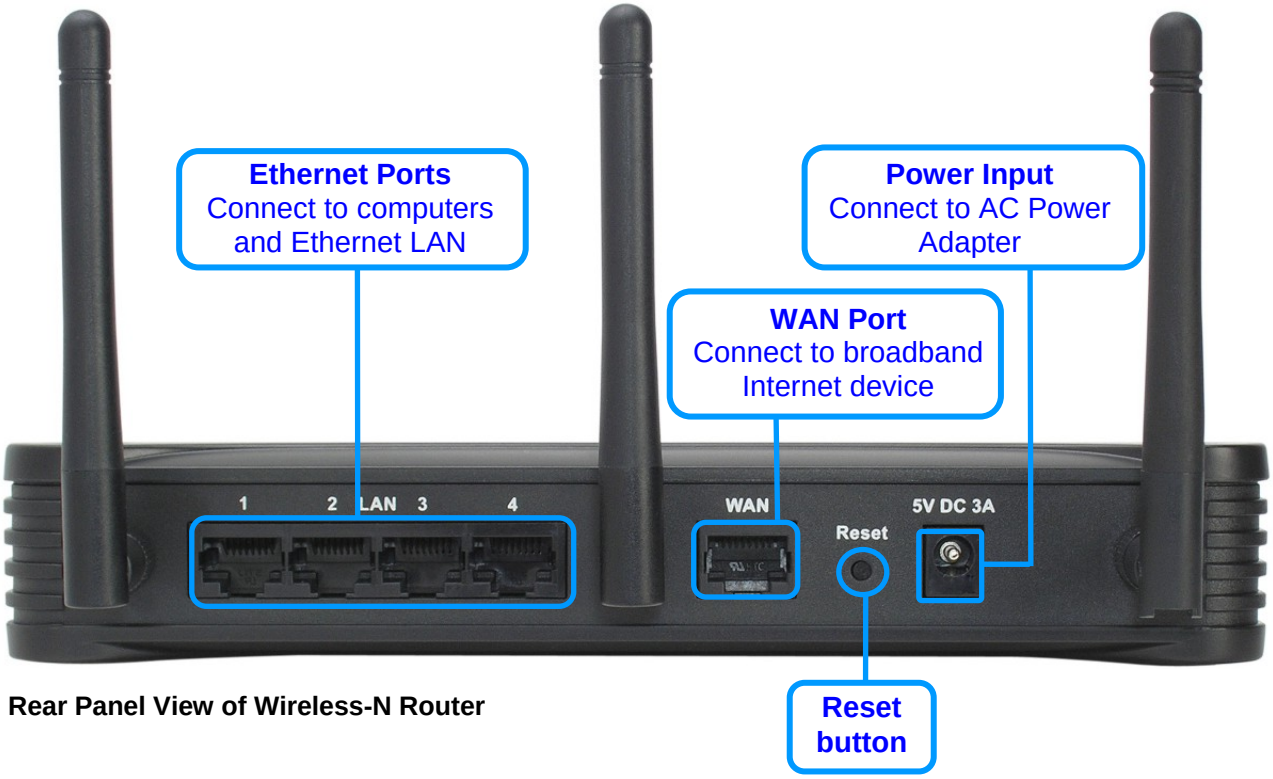
Place the router in a location that permits an easy view of the LED indicators on the front of the device.

The LED indicators include the **WPS**, **LAN**, **WLAN**, **WAN**, **Status** and **Power** indicators. The **WLAN** and Ethernet indicators monitor link status and activity (Link/Act).

WPS	Blinks blue for 120 seconds while searching for WPS enabled station. See Wi-Fi Protected Setup (WPS) for more information.
LAN (1-4)	A solid green light indicates a valid link on startup. This light blinks when there is activity currently passing through the Ethernet ports.
WLAN	Steady green light indicates a wireless connection. A blinking green light indicates activity on the WLAN interface
WAN	Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator lights steady green after the POST, the system has failed and the device should be rebooted.
Status	Blinks green when system function is normal.
Power	Steady green light indicates the unit is powered on. When the device is powered off this remains dark.

Rear Panel Connections

All cable connections to the router and the power adapter connect at the rear panel. Use the Reset button to restore the settings to the factory default values. See the next section for instructions to connect the power adapter and power on the router.



Rear Panel View of Wireless-N Router

CAUTION: Using a power supply with a different voltage rating will damage the device and void the warranty of this product.

Connecting Devices to the Router

The Wireless-N Router connects three separate networks, a private Ethernet LAN, Wireless LAN and the public Internet (WAN). Choose a location for the router where Ethernet devices can be connected to the LAN ports and the WAN port can be easily connected to the cable modem or DSL modem that provides the broadband Internet connection. Typically the broadband device is configured as a bridge, however some devices allow for more complex options. Consult the user manual of the broadband device for more information on how best to configure the broadband Internet connection.

The router should be protected from dust, water, moisture and heat. Make sure network cables, power adapters and power cords are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

Place the router on a shelf, desktop, or other secure stable platform. Ideally you should be able to view the LED indicators on the front panel.

Connect Router to Ethernet

The router can be connected to computers or other Ethernet devices using the four Ethernet LAN ports on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the router to any Ethernet device capable of operating at speeds between 10~100Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard CAT5 or better Ethernet cable with RJ-45 connectors. The Ethernet LAN ports are auto MDI-II/MDI-X so you can use straight-through or crossover Ethernet cabling.

The rules governing Ethernet cable lengths apply to the LAN to router connection. Be sure the Ethernet cables connected to the LAN ports do not exceed 100 meters in length.

Connecting through 802.11 Wireless

The default wireless settings of the access point allow roaming 802.11g and 802.11b wireless clients to associate with it. The first time you set up the router however, use the Ethernet connection to configure the channel and SSID. For wireless client-to-Internet connection through the router, first configure the Internet connection through the Ethernet. When the Internet connection has been established, make sure the wireless clients are configured as DHCP clients if you are using the router's DHCP server. Otherwise, make certain the wireless clients have IP settings that allow them to use the router as a gateway to the Internet.

General Guide to Setting Up a Wireless Network

In order to get the best performance from the wireless component of the router, you should have some basic understanding of how wireless networks operate. Wireless networking is a relatively new technology and there are more factors to consider when setting up or designing a wireless network than designing a wired network. If you are setting up a wireless network, especially if you are using multiple access points and/or covering a large area, good planning from the outset can ensure the best possible reliability, performance, coverage and effective security.

Radio

Wireless local network (as called WI-FI) devices such as notebook computers and wireless access points use electromagnetic waves within a broad, unlicensed range of the radio spectrum (between 2.4GHz and 2.5GHz) to transmit and receive radio signals. A wireless access point (AP) becomes a base station for the wireless nodes (notebook computer for example) in its

broadcast range. Often a wireless access point such as the AP embedded in the Wireless-N Router, will also provide a connection to a wired network - usually Ethernet - and ultimately an Internet connection. The IEEE 802.11 standard precisely defines the encoding techniques used to digitally used for data transmission. The embedded wireless access point can be used by IEEE 802.11g, 802.11b and 802.11n devices. These standards are compatible but use different algorithms for data transmission.

802.11g uses a method called Orthogonal Frequency Division Multiplexing (OFDM) for transmitting data at higher data rates. OFDM is a more efficient encoding method than Direct Sequence Spread Spectrum (DSSS) transmission, the method used by 802.11b devices. However, in order to support different data transmission rates while also be compatible with 802.11b, 802.11g uses a combination of OFDM and DSSS when 802.11b devices are present.

Range

An access point will send and receive signals within a limited range. Also, be aware that the radio signals are emitted in all directions giving the access point a spherical operating range. The physical environment in which the AP is operating can have a huge impact on its effectiveness. If you experience low signal strength or slow throughput, consider positioning the router in a different location. See the discussion below concerning the wireless environment and location of the AP (Wireless-N Router).

SSID and Channel

Wireless networks use an SSID (Service Set Identifier) as means of identifying a group of wireless devices, similar to a domain or subnet. This allows wireless devices to roam from one AP to another and remain connected. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network.

The embedded wireless access point of the router operates in *Infrastructure* mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. By default, the Wireless-N Router broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate. You may disable SSID broadcasting in the web manager’s wireless menu.

In addition, the AP can use different channels (frequency bands) to avoid unwanted overlap or interfere between control zones of separate APs. Wireless nodes must use the same SSID and the same channel as the AP with which it wishes to associate. However, because of the nature of the CSMA/CA (carrier sense multiple access with collision avoidance) protocol, using the same channel on two different APs can contribute significantly to wireless congestion. If you are using multiple APs on your network and are experiencing low throughput or significant transmission delay, carefully consider how channels are assigned to the different APs.

Wireless Security

Various security options are available on the Wireless-N Router including open or WEP and WPA (including WPA-PSK). Authentication may use an open system or a shared key. Read below for more information on configuring security for the wireless interface.

Installation Considerations for Wireless LAN

Many physical environmental factors can impact wireless networks. Radio waves are used to carry the encoded data between devices. These radio transmissions can become degraded due to signal attenuation, multi-path distortion and interference or noise. Attenuation simply means that the strength of the signal weakens with the distance it travels, even if the transmission path is unobstructed. Multi-path distortion occurs when radio signals bounce off objects like walls, ceilings, metal appliances, etc. This may cause a signal to be duplicated, with each separate yet identical signal arriving at a receiver at different times. Interference and noise from electrical devices such as microwave ovens, fluorescent lights, automobile engines and other radio emitting devices can cause signal degradation. With all of this in mind, choose a location for all access points on the wireless LAN.

Wireless networking lets you access your network from nearly anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. To maximize range and signal strength, use these basic guidelines:

- Keep the number of walls and ceilings between the access point and other network devices to a minimum - each wall or ceiling can reduce your wireless device's range from 3-90 feet (1-30 meters.) Position wireless devices so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not dense, especially metallic, materials. Also, note that metal filing cabinets and appliances can reflect radio signals. When these metal objects are moved around, your wireless network may be affected.
- Keep your access point away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise such as microwave ovens, CRT monitors, motors, etc.

Power on Wireless–N Router

CAUTION: The Wireless-N Router must be used with the power adapter included with the device. Using a power supply with a different voltage rating will damage and void the warranty for this product

To power on the Wireless-N Router:

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Wireless-N Router and plug the adapter into a suitable nearby power source. See the back panel illustration above to view the power receptacle.

2. The Power LED indicator will immediately light green and remain lit. The Status LED should light steady green initially and begin to blink after a few seconds.

3. If an Ethernet port is connected to a computer or other device, look at the Ethernet Link/Act LED indicators to make sure they have valid connections. The Wireless Broadband Router will attempt to establish the WAN connection, if the WAN line is connected and the connection is properly configured the WAN LED indicator will light up after several seconds.

Factory Reset Button

The Wireless-N Router may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address **192.168.1.1** and the subnet mask is **255.255.255.0**, the default management Username is **admin** and the default Password is **admin**.

The router may also be reset to factory default configuration settings through the web management interface.

Configuration

All device configuration for the router is done through the web-based management software. Use a standard web browser with JavaScript enabled to connect to the web manager. Make sure the proxy settings for the browser do not require use of a proxy server.

IP Settings on Your Computer

In order to configure your system to receive IP settings from the router it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. The DHCP server will automatically enable your computer to use a browser to manage the router. Configuring IP Settings on Your Computer on page 71 describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client. If you are running another operating system, make sure your computer is configured as a DHCP client so it can automatically obtain IP settings from the router. Some operating systems will automatically select the best IP settings. Consult the user manual for the operating system (OS) if you are unsure.

For computers using manually configured IP settings, make sure the IP address is on the same subnet as the router. The computer should use an IP address in the range 192.168.1.2 to 192.168.1.254 with a subnet mask of 255.255.255.0.

NOTE: If you are not sure how to configure your Windows computer to be a DHCP client, see Configuring IP Settings on Your Computer in Configuring IP Settings on Your Computer.

Access the Configuration Manager

In order to make sure your computer's IP settings allow it to communicate with the router, it is advisable to configure your system be a DHCP client – that is, it will get IP settings from the router. Configuring IP Settings on Your Computer on page 71 describes how to configure different Windows operating systems to "Obtain IP settings automatically".

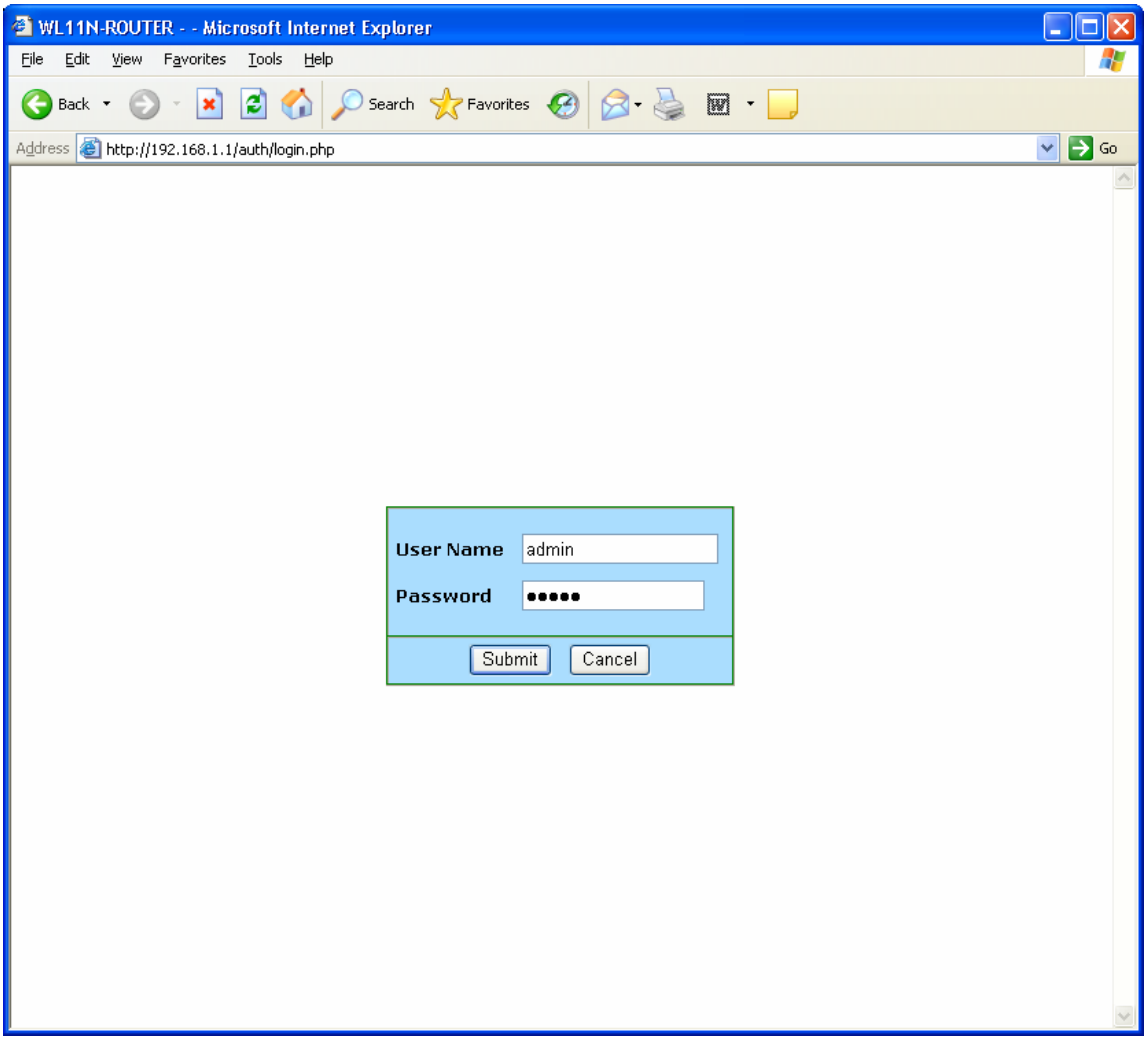
Be sure that the web browser on your computer is not configured to use a proxy server in the Internet settings. In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:

1. In Windows, click on the **Start** button and choose **Control Panel**.
2. In the **Control Panel** window, click on the **Network and Internet Options** icon.
3. In the **Network and Internet Connections** window, click the **Internet Options** icon.
4. In the **Internet Properties** window, click on the **Connections** tab and click on the **LAN Settings** button
5. Verify that the "Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)." option is NOT checked. If it is checked, click in the checked box to deselect the option and click **OK**.

Alternatively, you can access this **Internet Options** menu using the **Tools** pull-down menu in Internet Explorer.

Login to Home Page

To use the web-based management software, launch a suitable web browser and direct it to the IP address of the router. Type in **http://** followed by the default IP address, **192.168.1.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.1.1**. Type in the default User Name admin and the default Password admin then click the **Submit** button to access the web-based manager.

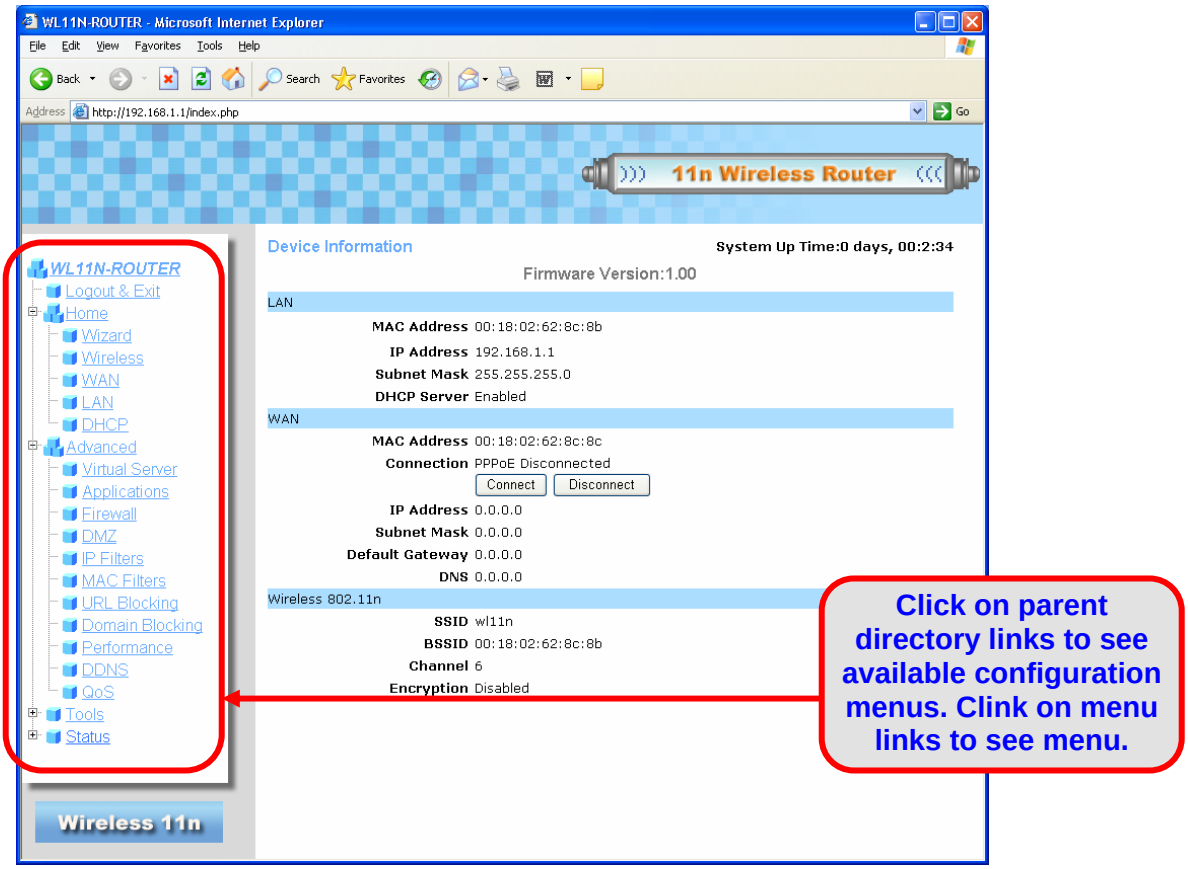


Enter Password

It is recommended to change the web-based manager access user name and password once you have verified that a connection can be established. The user name and password allows any PC within the same subnet as the router to access the web-based manger.

Web Manager

When you successfully connect to the web manager, the **Device Information** display in the **Status** menu directory is displayed. For quick configuration of the Internet connection, launch the Setup Wizard in the Home directory.



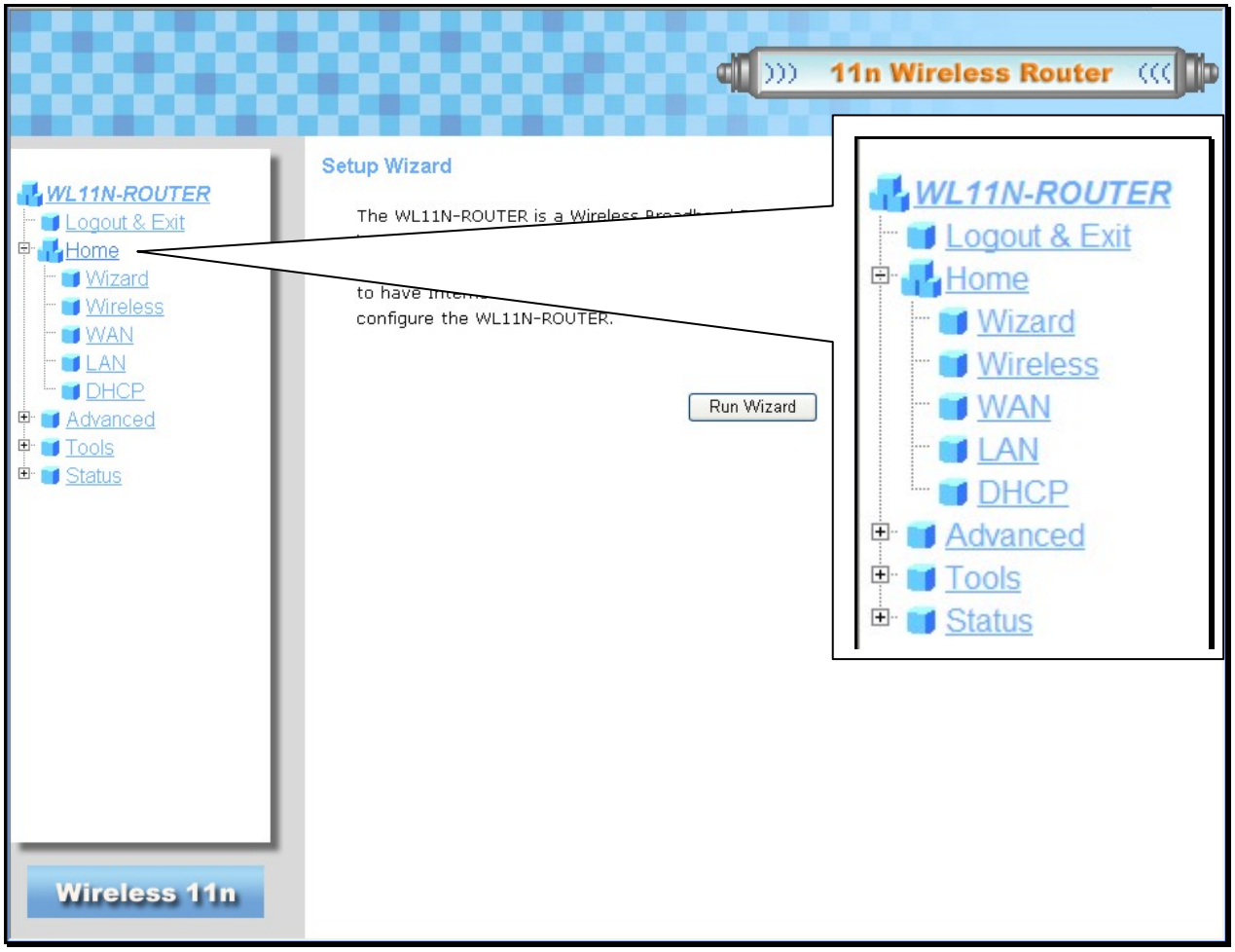
Web Manager – First Time Log On

All configuration and management of the router is done using the web-based management interface. To view the menus contained in each menu directory, click the + symbol to expand the menu tree.

Parent Directory	Configuration and Read-only menus
Home	Click the Home link to access the Setup Wizard and the menus used to configure the basic router settings. The Home directory menus are Wizard, Wireless, WAN, LAN and DHCP.
Advanced	Click the Advanced link to access the Virtual Server, Applications, Firewall, DMZ, IP Filters, MAC Filters, URL Blocking, Domain Blocking, Wireless Performance, DDNS and QoS menus.
Tools	Click the Tools link to access the Administrator (used to set the system password), Time, System, Firmware and Miscellaneous menus.
Status	Click the Status link to view the DHCP Clients, View Log, Wireless Clients and Statistics displays.

Basic Configuration – Home Directory Menus

The first time you setup the router it is recommended that you configure the WAN connection using a single computer making sure that both the computer and the router are not connected to the Ethernet LAN or other Ethernet devices. Once the Internet connection is configured and working, go ahead and connect other Ethernet and wireless devices.

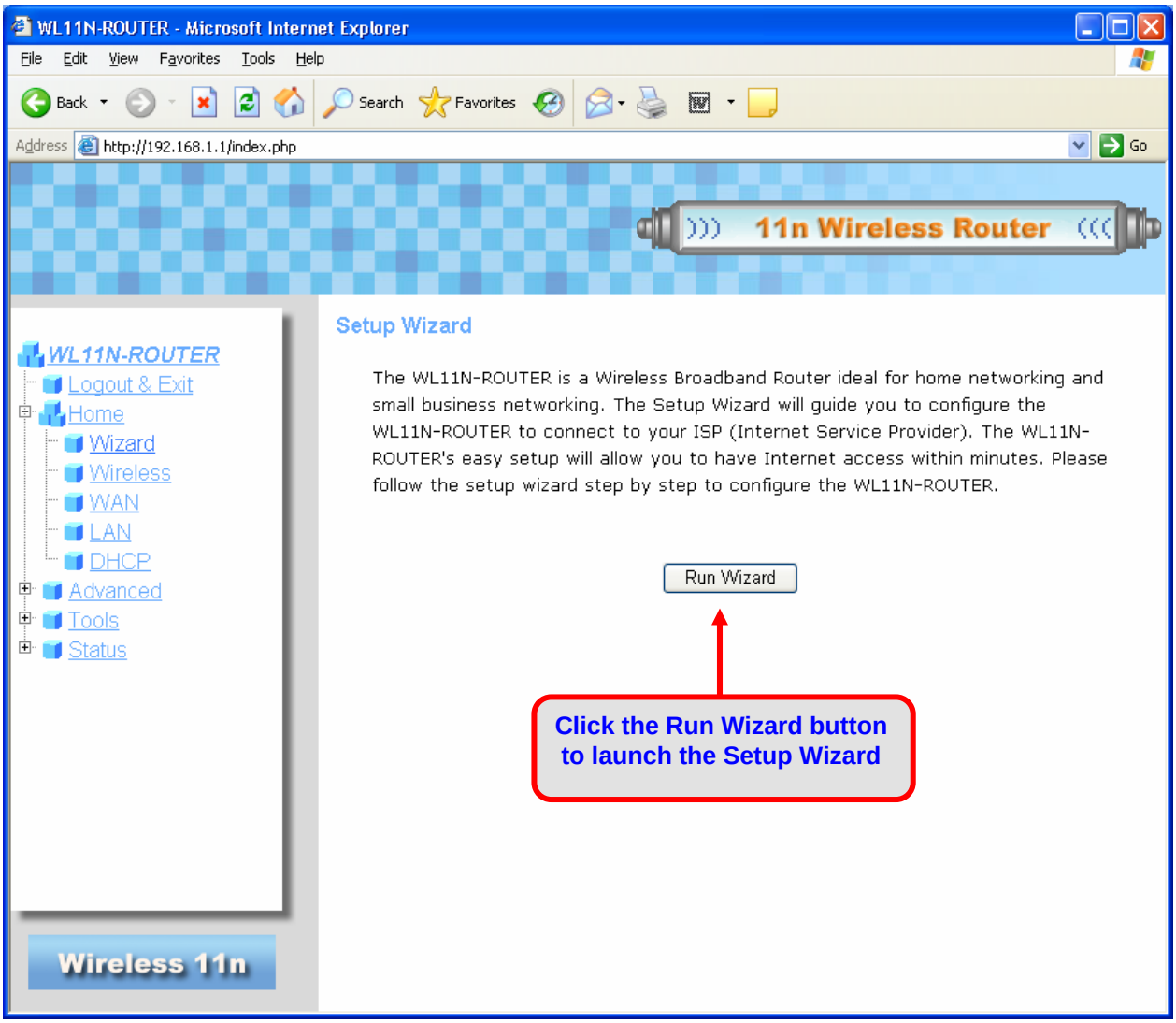


Home Directory Menus

The Setup Wizard page is the first page to appear when clicking on the Home directory link.

Setup Wizard

To use the Setup Wizard, click the **Run Wizard** button in the first browser window that appears in the Home directory and follow the instructions in the pop-up window that appears.



Launch Setup Wizard

Follow the instruction below to the type of connection used for your broadband Internet connection.

Using the Setup Wizard

The initial window summarizes the setup process. Click the **Next** button to proceed. You may stop using the Setup Wizard at any time by clicking the **Exit** button. If you exit the wizard you will return to the **Setup Wizard** window without saving any of the settings changed during the process.

The first pop-up window of the Setup Wizard lists the basic steps in the process. These steps are as follows:

1. Set the system password
2. Set the system time.
3. Configure the connection to the Internet.
4. Set the wireless configuration.
5. Save the new configuration settings and reboot the system.

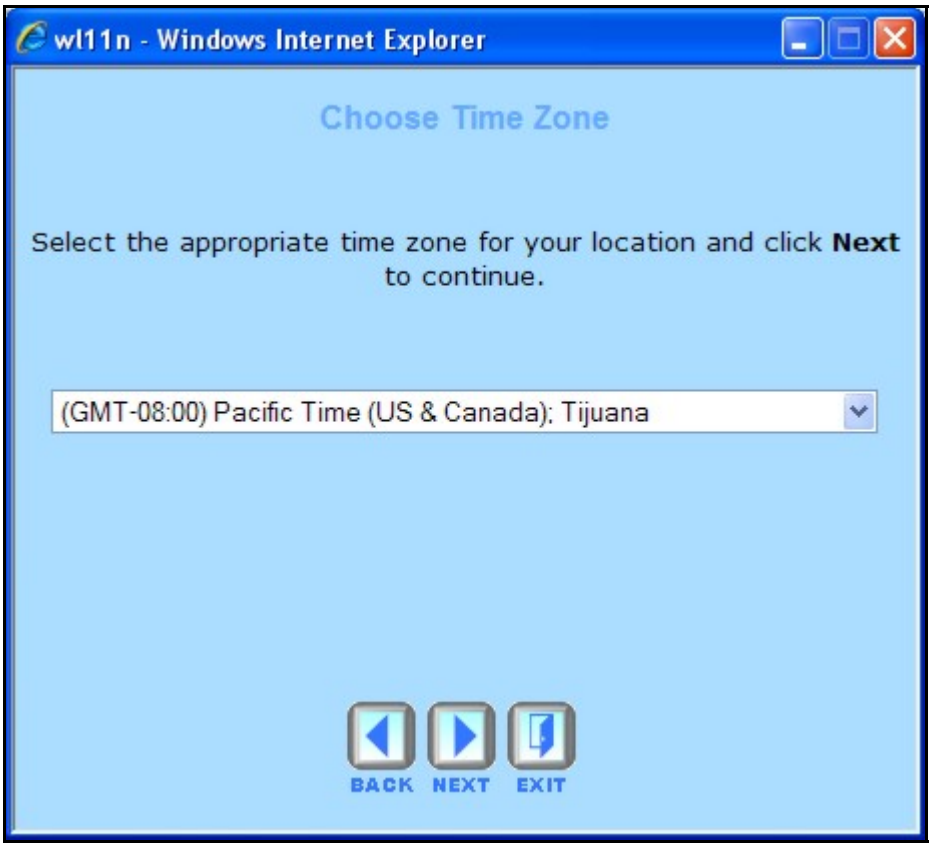
Using the Setup Wizard- Set System Password

Change the password used for management access of the router. Type the new **Password** and **Confirm** it in the spaces provided. Click the **Next** button to proceed.

NOTE: The System user name “admin” cannot be changed.

Using the Setup Wizard - Choose Time Zone

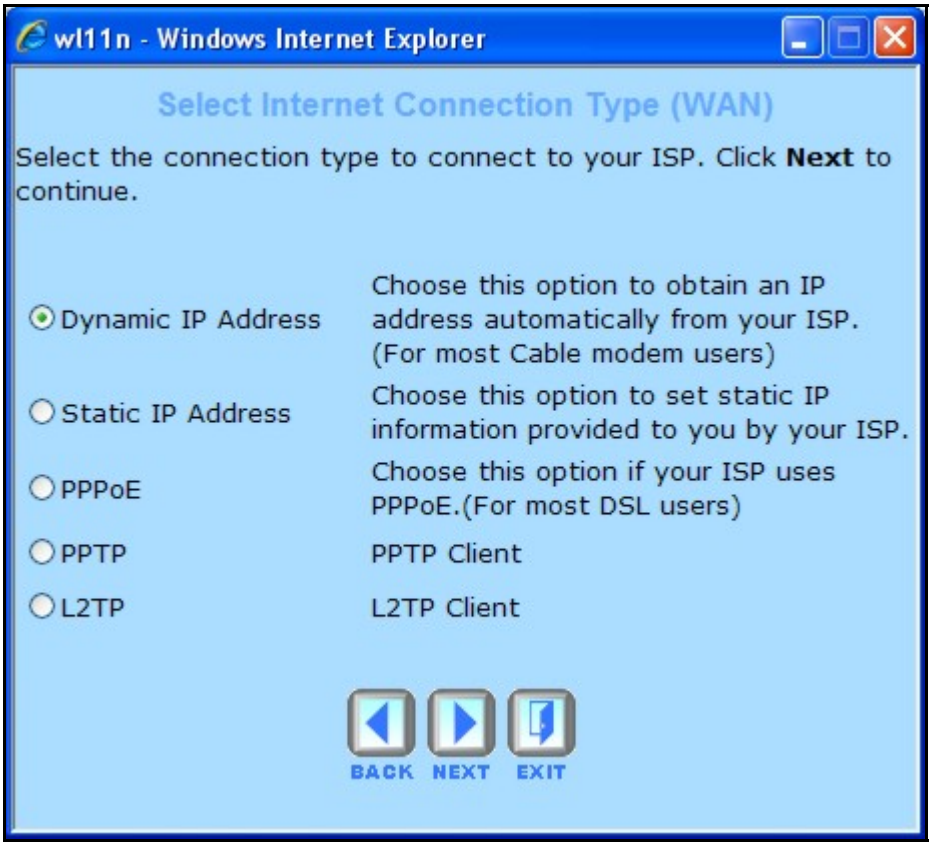
Choose the time zone you are in from the pull-down menu and click **Next**. This sets the system time used for the router. If you wish to return to the previous window during the setup process, click the **Back** button.



Select the **Connection Type** specific to your service and click **Next** to go to the next **Setup Wizard** window. Follow the instructions below for the type of connection you have selected.

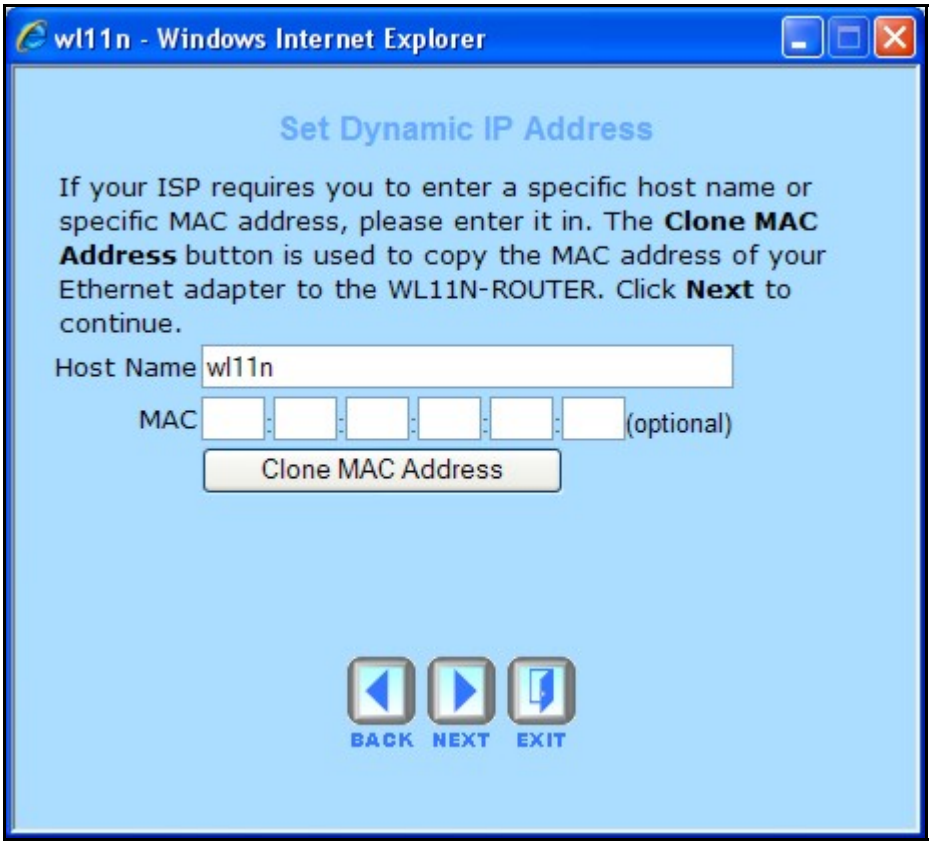
Using the Setup Wizard - Choose Connection Type

Now select the Connection Type used for the Internet connection. Your ISP has given this information to you. The connection types available for are **Static IP**, **Dynamic IP**, **PPPoE**, **PPtP** and **L2tP**. Each connection type has different settings that are configured in the next **Setup Wizard** window.



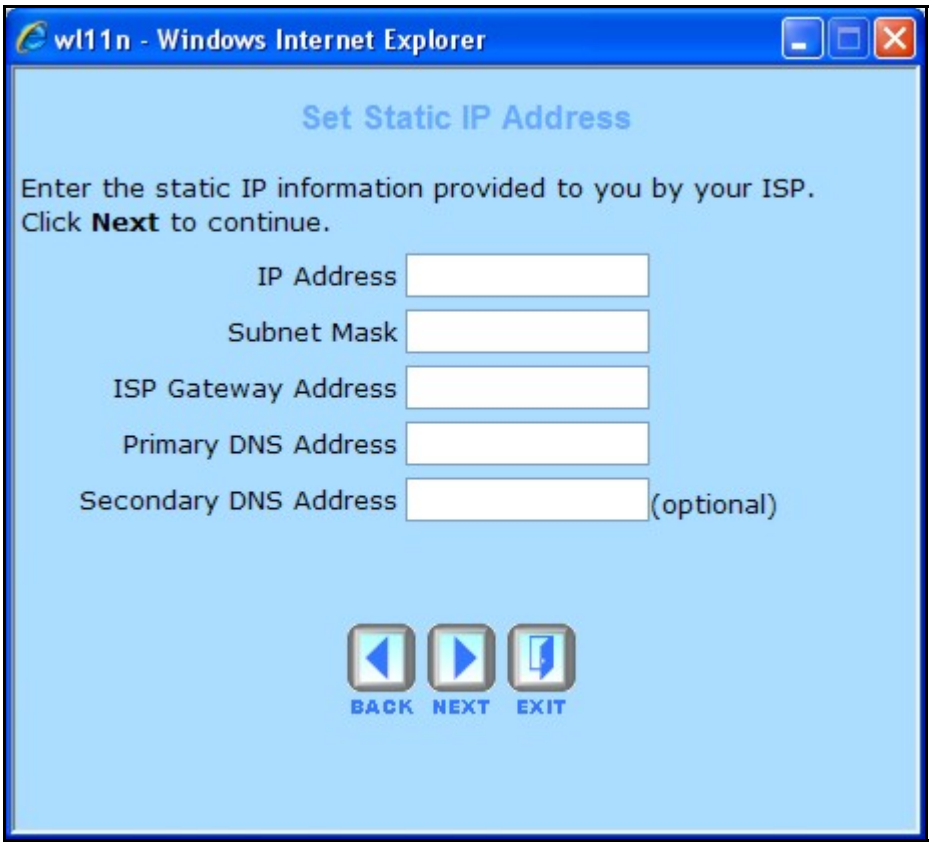
Using the Setup Wizard - For Dynamic IP Address connections:

1. Select the specific **Connection Type** from the drop-down menu. The available Dynamic IP Address connection and encapsulation types are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*.
2. If you are instructed to change the **VPI** or **VCI** number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.
3. You may want to copy the MAC address of your Ethernet adapter to the router. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. This can prevent the router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the Cloned MAC Address field and click the **Clone MAC Address** button. This will copy the information to a file used by the router to present to the ISP's server used for DHCP.
4. Click **Next** to go to the **Set Wireless LAN Connection** pop-up window.



Using the Setup Wizard - For Static IP Address connections:

1. Select the specific **Connection Type** from the drop-down menu. The available Static IP Address connection and encapsulation types are *1483 Bridged IP LLC*, *1483 Bridged IP VC-Mux*, *1483 Routed IP LLC*, *1483 Routed IP VC-Mux* and *IPoA*.
2. Change the **IP Address**, **Subnet Mask**, **ISP Gateway Address**, **Primary DNS Address**, and **Secondary DNS** Server IP **Address** as instructed by your ISP. For IPoA connections it may also be necessary to change the **ARP Server Address**. IPoA connection users who have not been given this information should leave the field blank.
3. If you are instructed to change the **VPI** or **VCI** number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.
4. Click **Next** to go to the **Set Wireless LAN Connection** pop-up window.

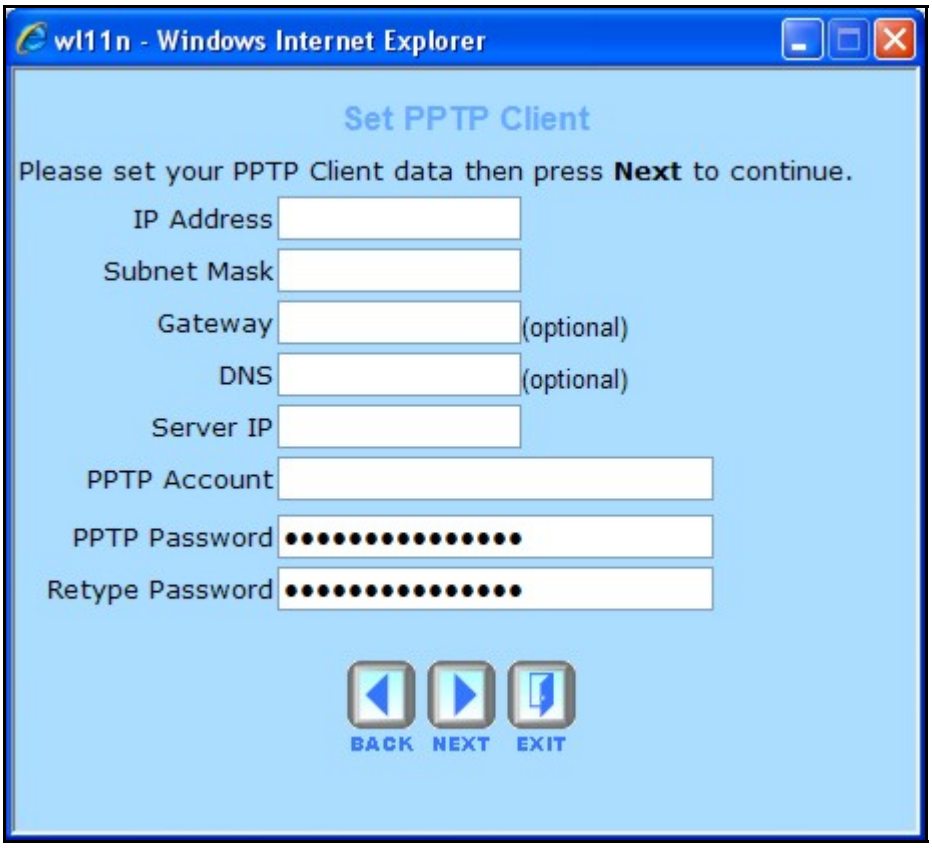


Using the Setup Wizard - For PPPoE connections:

1. Type in the **Username** and **Password** used to identify and verify your account to the ISP. **Retype** the password to make sure it is correct.
2. Click **Next** to go to the **Set Wireless LAN Connection** pop-up window.

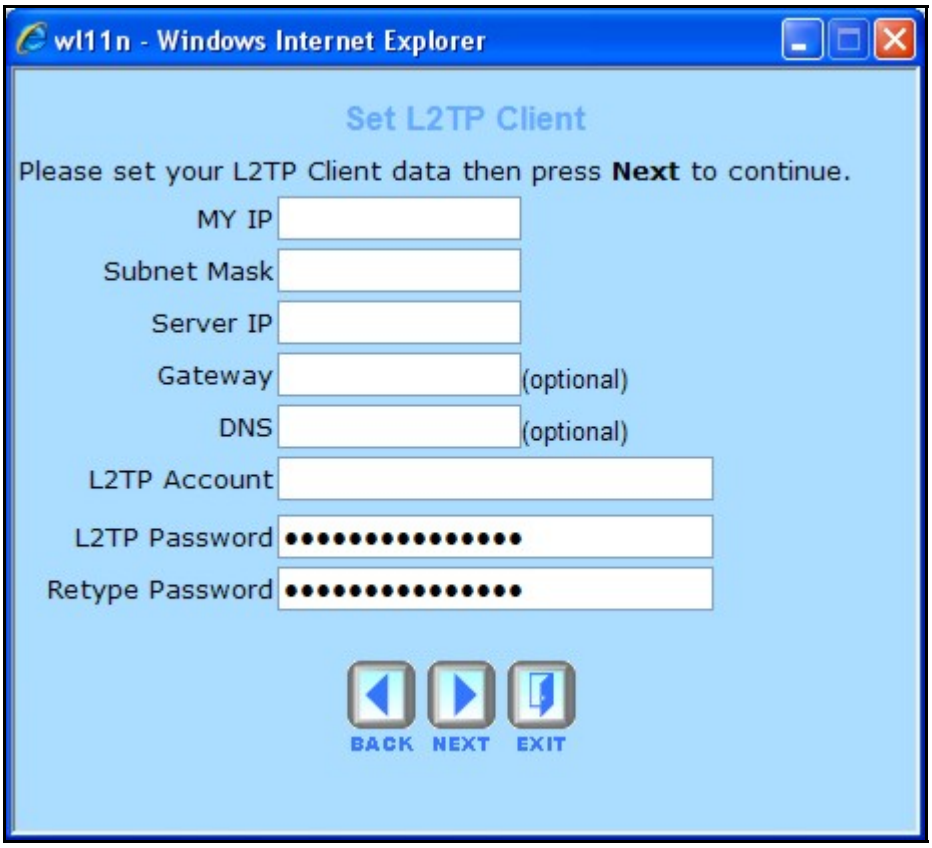
Using the Setup Wizard – For PPTP Client connections:

1. Enter the appropriate PPTP Client information including PPTP **Server IP**, **PPTP Account** name, and the **PPTP Password** twice.
2. Click **Next** when you are ready to continue to the **Set 802.11g Wireless LAN Configuration** window.



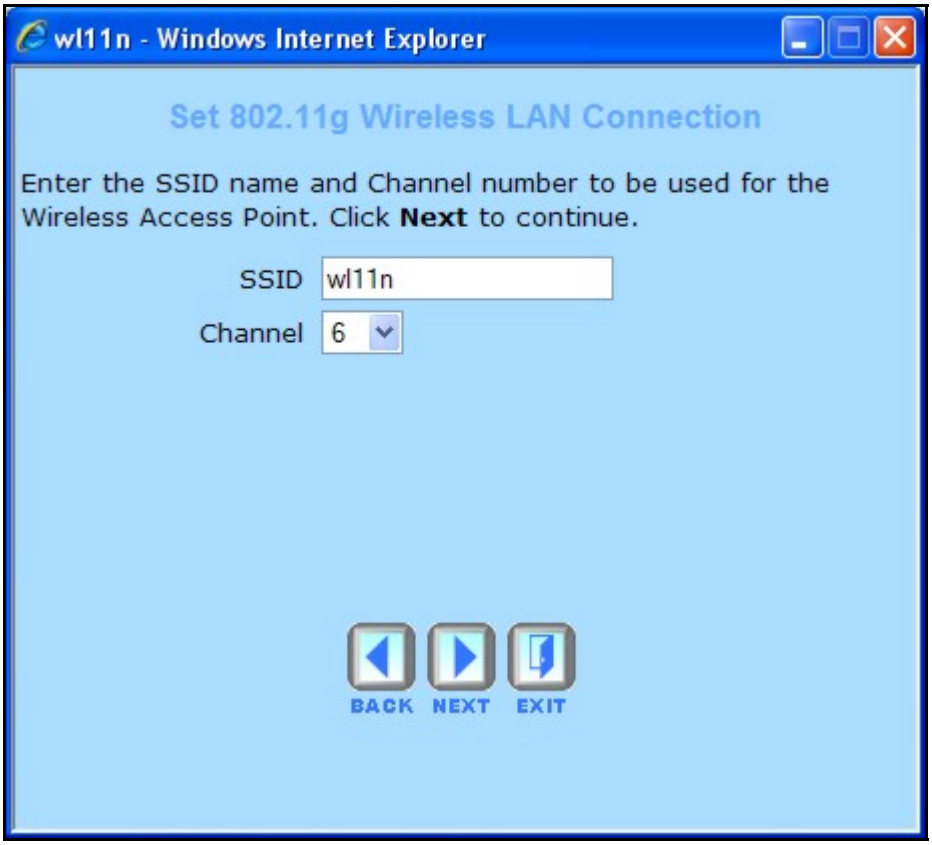
Using the Setup Wizard – For L2TP Client connections:

1. Enter the appropriate L2TP Client information including L2TP **Server IP**, **L2TP Account** name, and the **L2TP Password** twice.
2. Click **Next** when you are ready to continue to the **Set 802.11g Wireless LAN Configuration** window.



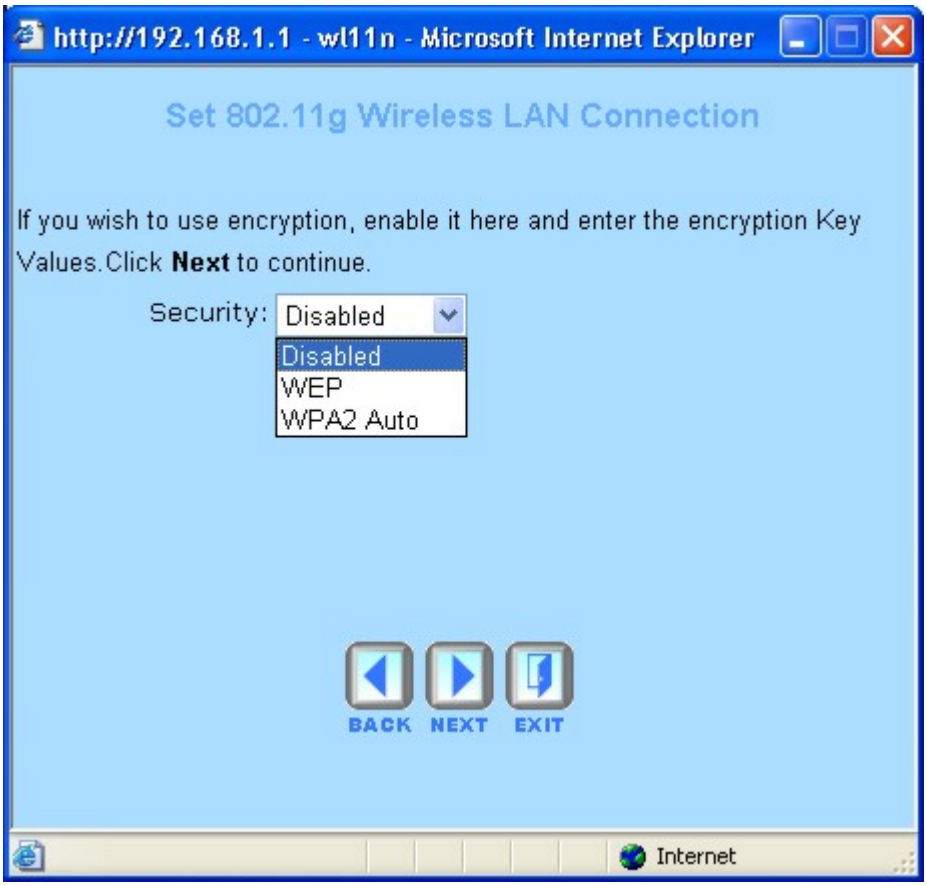
Using the Setup Wizard - Wireless LAN connection:

1. The **SSID** identifies members of the Service Set. Accept the default name or change it to something else. If the default SSID is changed, all other devices on the wireless network must use the same SSID.
2. The wireless **Channel** number is available from your Internet Service Provider (ISP). What channels are available for use by the access point depends on the local regulatory environment. Remember that all devices communicating with the device must use the same channel (and use the same SSID). Use the drop-down menu to select the channel used for your 802.11 Wireless LAN.
3. Click **Next** to go to the next window.



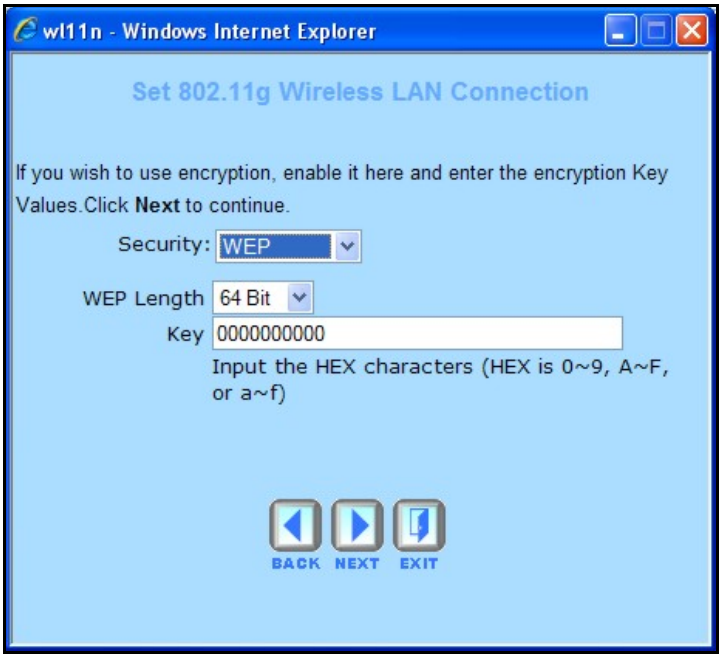
Using the Setup Wizard - Wireless LAN security:

Wireless LAN security supported includes WEP and WPA versions 1 and 2. Select the preferred method from the list and click on the **Next** button. You can choose to setup security later, in which case choose the Disabled option. If you choose to leave security disabled at this time, the next menu will be the Save and Take Effect wizard menu.



Using the Setup Wizard – WEP Configuration

The Setup Wizard wireless LAN security configuration is limited to WEP; for WPA or WPA2 security, use the web-based manager Wireless Settings menu. To configure WEP in the Setup Wizard, select Open, Shared or Both for Authentication Type, use the Cipher: pull down menu to select the level of encryption or cipher rate, 64 bits or 128 bits and type in an encryption key of appropriate length. For 64-bit encryption, type a key ten hexadecimal digit (0~9,A~F) key, for 128-bit encryption type a 26 hexadecimal digit key.

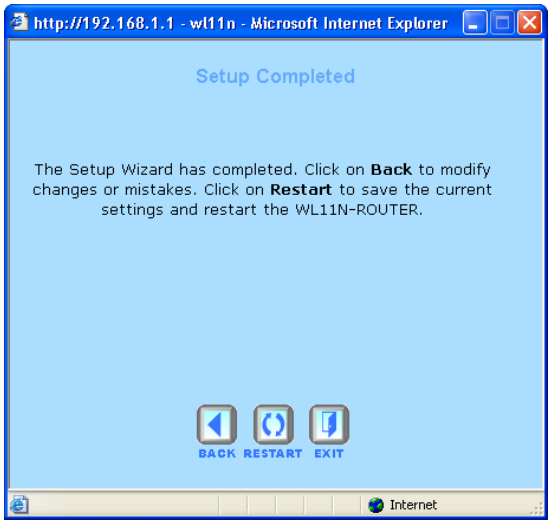


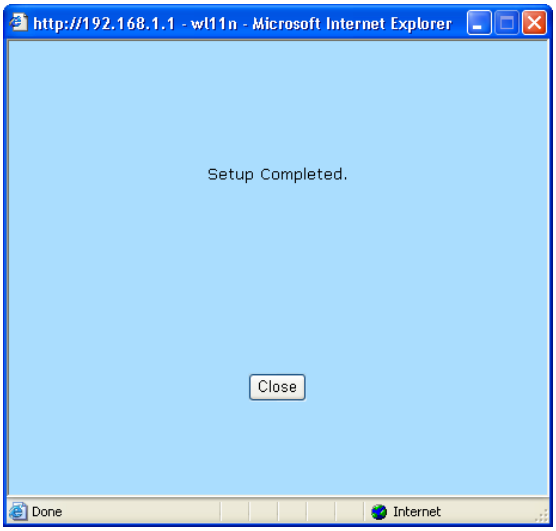
Using the Setup Wizard – WPA2 Auto Configuration

If you are configuring WPA security, select **Security** type WPA2 Auto, enter the **Passphrase** used for authentication. Click **Next** to continue to the final menu.

Using the Setup Wizard - Finish and Restart

Finally you can confirm that the setup process is completed. If you are satisfied that you have entered all the necessary information correctly, click the **Restart** button to save the new configuration settings and restart the router. If you need to change settings from a previous window, click the **Back** button.

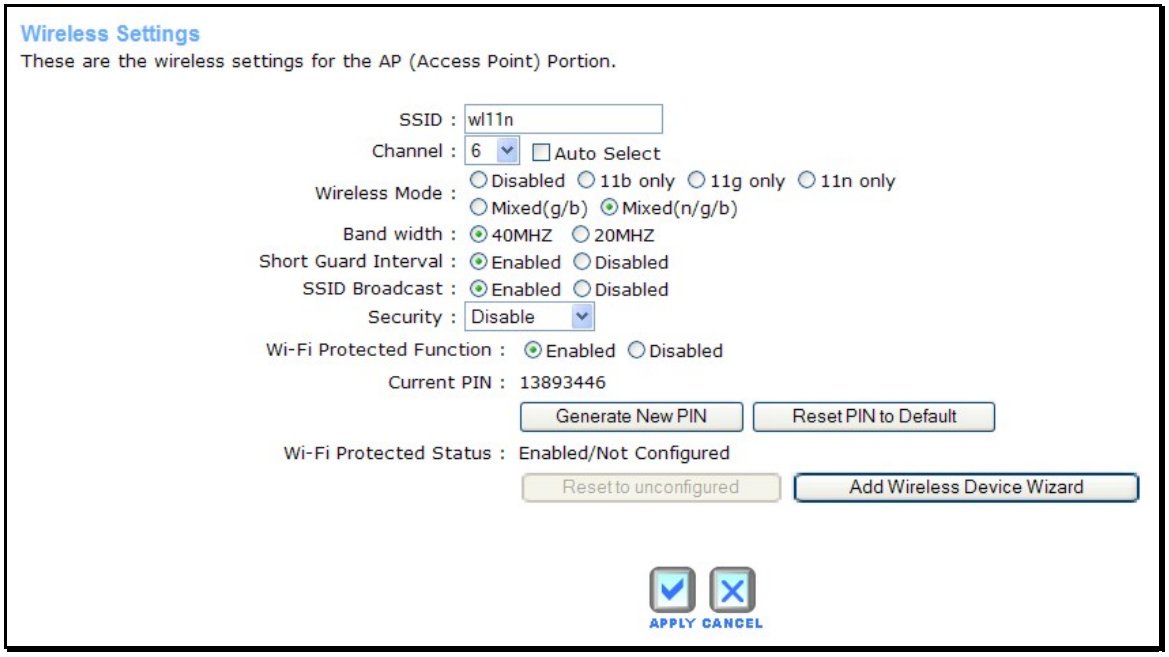




CAUTION: Do not turn the router off while it is restarting. After the router is finished restarting, you are now ready to continue to configure the router as desired. You may want to test the WAN connection by accessing the Internet with your browser.

Basic Wireless Setup

To configure the router's basic wireless and wired network configuration settings without running the Setup Wizard, you can access the windows used to configure Wireless, WAN, LAN and DHCP settings directly from the **Home** directory. To access the **Wireless Settings** window, click on the **Wireless** link on the left side of the first window that appears when you successfully access the web manager.



Wireless Settings menu – default settings

By default the wireless AP is enabled for use by 802.11b, 802.11g and 802.11n workstations. The **Set Wireless Mode** options are used to configure the access point to use 11b only, 11g only, 11n only, a mix of 11b and 11g, or a mix of all three standards. To turn off all wireless function, select the *Disable* option.

The **SSID** identifies members of the Service Set. Accept the default name or change it to something else. All other devices on the wireless network using the Wireless Broadband Router must use the same SSID.

What channels are available for use by the access point depends on the local regulatory environment. Remember that all devices communicating with the device must use the same channel (and use the same SSID). Use the drop-down menu to select the **Channel** used for your 802.11 Wireless LAN. The wireless channel number is available from your Internet Service Provider (ISP).

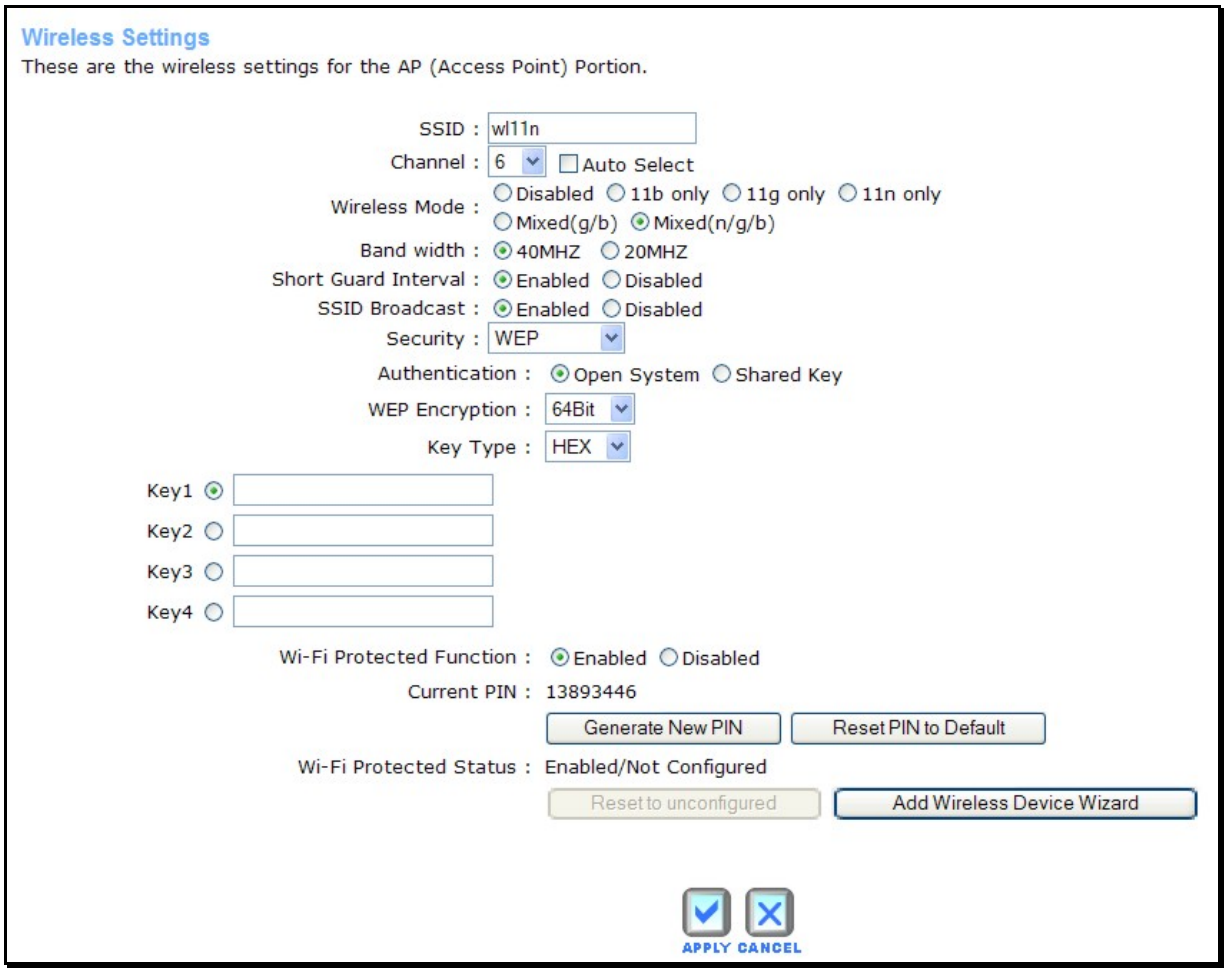
If network **Security** is not used, click None, then click **Apply**.

NOTE: For wireless stations that support WPS push button method, the easiest way to establish a secure connection is to simultaneously press the WPS button on the wireless workstation and the WPS button on the front of the Wireless Broadband Router. See below for more information on WPS.

Wi-Fi Protected Function is enabled by default. See below for more information on Wi-Fi Protected Status or WPS.

Wireless Security

In the **Wireless Settings** window, select the type of security you want to configure. The window will change to present the settings specific to the method being configured. The Wireless-N Router's wireless security options include three levels of WEP encryption, WPA for IEEE 802.1x network authentication, and WPA with a user-configured Pre Shared Key (PSK) or RADIUS authentication. The Wireless-N Router supports Wi-Fi Protected Setup (WPS) for quickly establishing a secure link to stations that support WPS. Enabling WEP or WPA security will automatically disable WPS function.



Wireless Settings window – WEP

Wireless bandwidth, Short Guard Interval and SSID Broadcast options are available for configuration for all security methods including WPS.

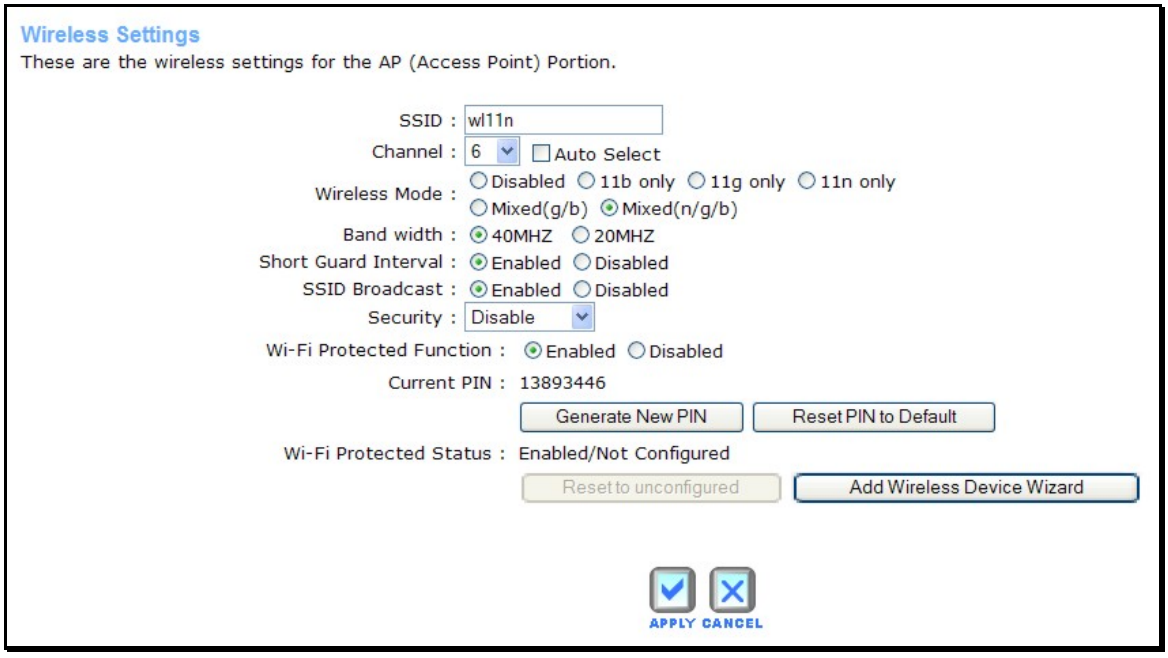
NOTE: Enabling WEP or WPA security will automatically disable WPS function.

Wi-Fi Protected Setup (WPS)

WPS provides an easy way to configure a secure connection to your wireless LAN. This option can be used on wireless stations that support Wi-Fi Protected Setup or WPS. The Wireless Broadband Router supports push button and PIN methods of WPS. WPS cannot be used with WPA or WPA2.

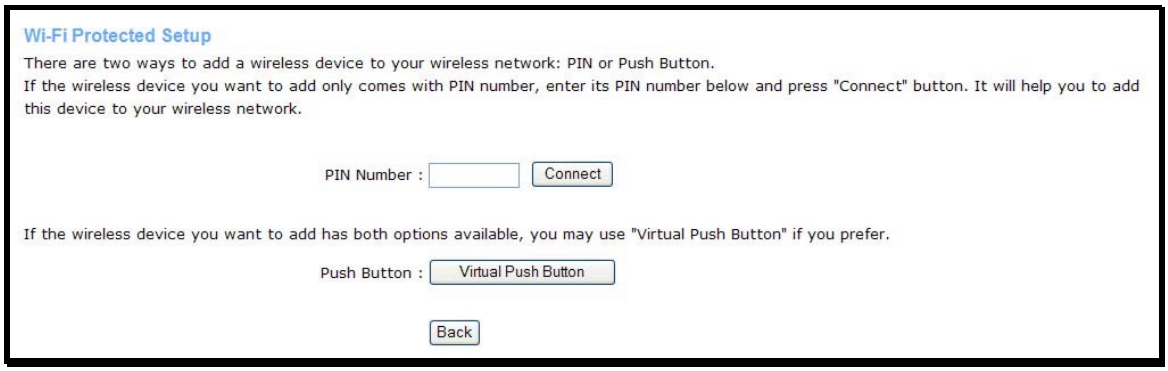
The WPS menu is located at the bottom of the Wireless menu. To use WPS click to select the **Enabled** radio button for **Wi-Fi Protected Function**.

NOTE: The **Generate New PIN** button is for the Wireless-N Router's own PIN. This is used when the router needs to connect to other WPS enabled access points.



Wireless Settings menu

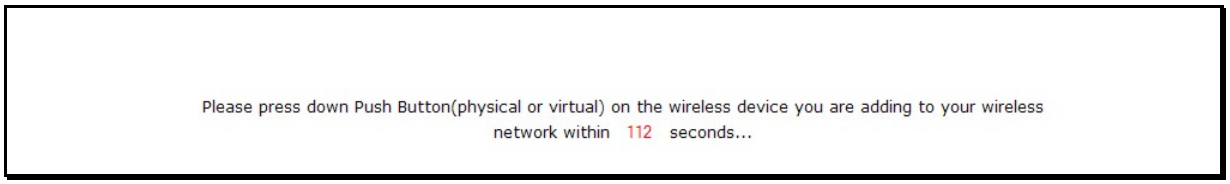
To add a wireless station using WPS, enter the PIN number of the WPS enabled wireless device and click on the **Connect** button.



WPS station PIN entry / Virtual Push Button menu

The router will attempt to establish the WPS secure connection for 120 seconds. Now start the WPS connection process on the device attempting to make the connection.

While the router is searching for the wireless station with the PIN just entered, a message informs you to start the WPS device.



WPS start PIN device message

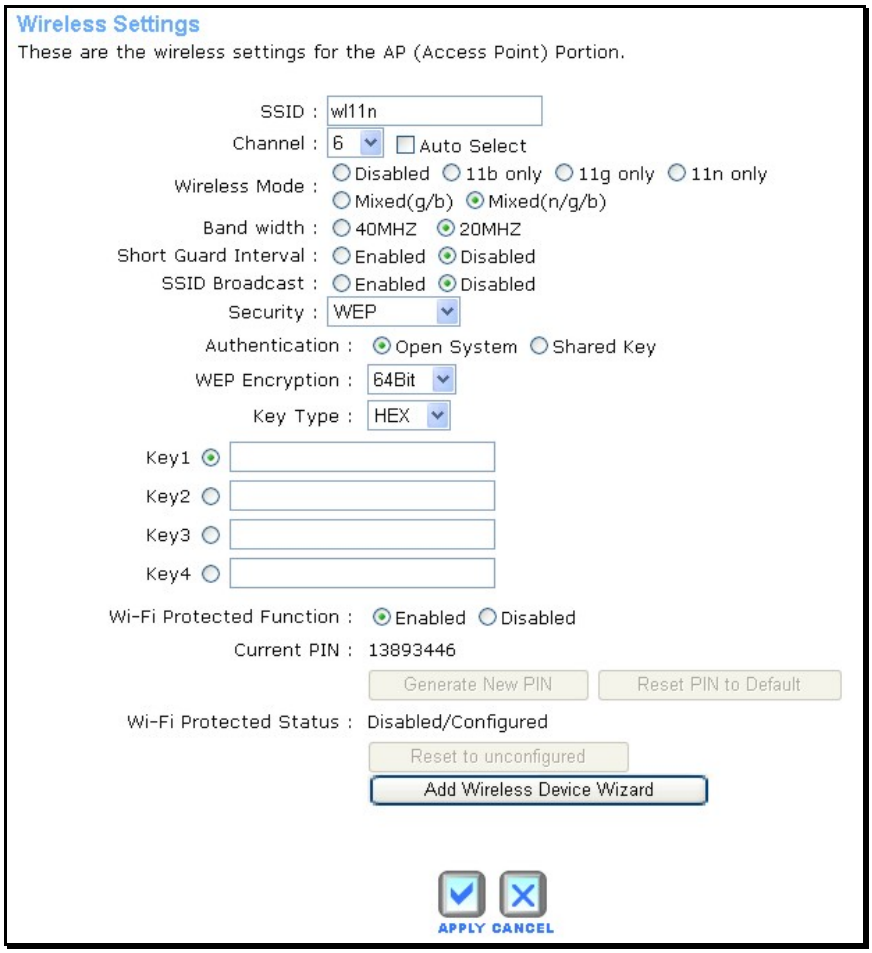
Alternatively, for wireless stations that support the push button WPS method, click on the **Virtual Push Button** or press the red WPS button on the front panel of the router to begin the WPS connection process.

WPS push button on WPS device message

The router will attempt to establish the WPS secure connection for 120 seconds. Press the button on the device trying to connect.

WEP Encryption

Use WEP encryption for basic wireless data encryption. Use WPA if wireless LANs that require a higher level of security. WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. The router offers 64 or 128-bit encryption with four keys available. Select the WEP option from the **Security:** pull-down menu to configure WEP encryption.



Wireless Settings menu – WEP encryption

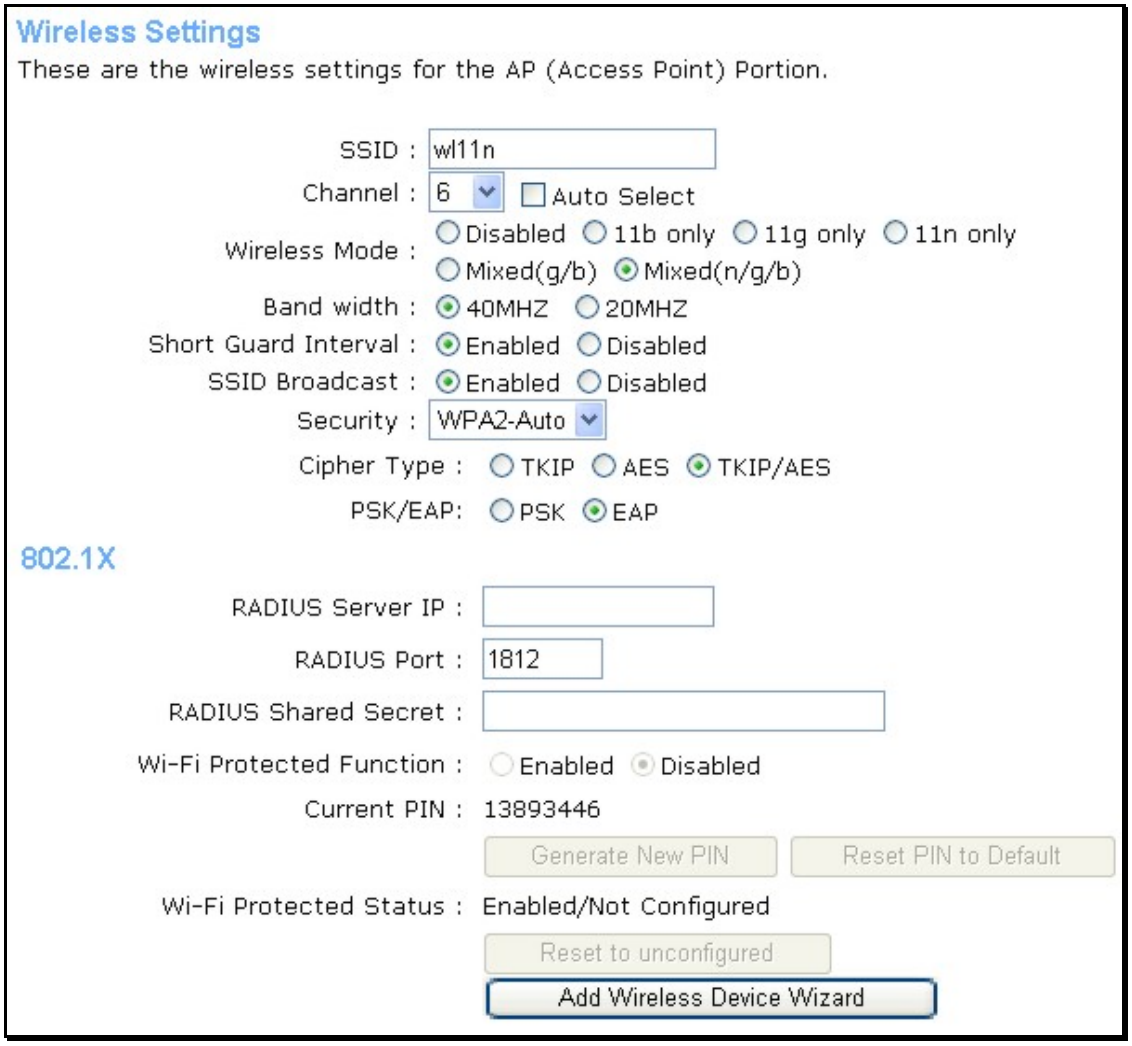
Enter the appropriate parameters for the type of security selected from this menu. WEP security requires the following:

- **Authentication Type:** Open Key or Shared Key.
- **Encryption Length:** The IP address of the RADIUS server.
- **Key Type:** ASCII or Hexidecimal.
- **Key:** Type up to four keys of appropriate length, 10 characters for 64-bit Hex or 26 characters for 128-bit Hex.

NOTE: If encryption of any kind, at any level is applied to the Wireless-N Router, all wireless devices using the router on the network must comply with all security measures.

WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP.



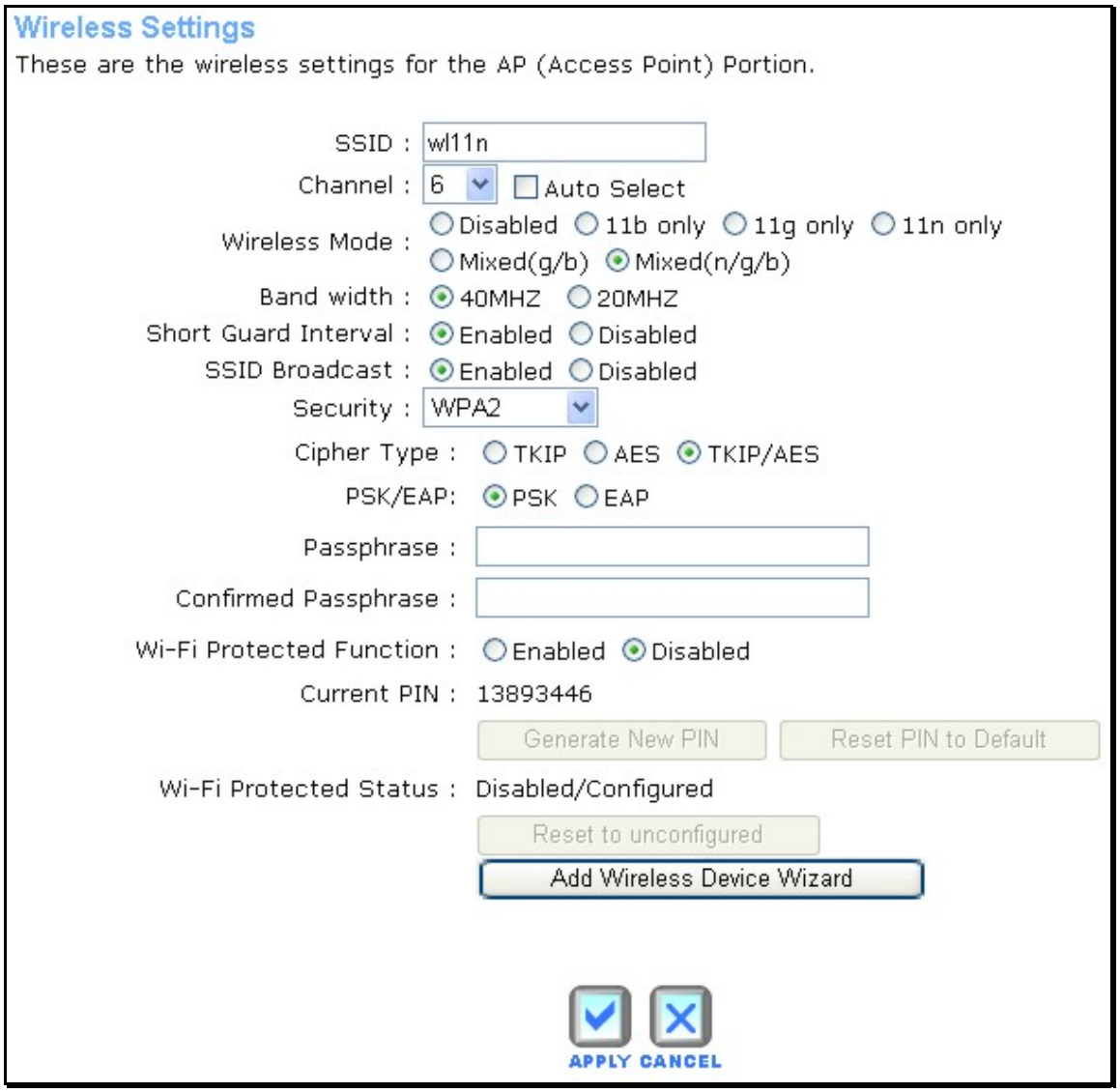
Wireless Settings menu – WPA2 EAP

Enter the appropriate parameters for the type of security selected from this menu. For EAP authentication using WPA or WPA2, enter the following:

- **Cypher Type:** Choose TKIP, AES or TKIP/AES.
- **RADIUS Server:** The IP address of the RADIUS server.
- **RADIUS Port:** The port number used for 802.1x.
- **Shared Key:** The password or character string used for wireless station authentication.
- **Key Renewal:** The time (in seconds) after which the Shared Key is changed automatically.

NOTE: If encryption of any kind, at any level is applied to the Wireless-N Router, all wireless devices using the router on the network must comply with all security measures.

Select the PSK authentication option to view the WPA passkey configuration menu.



Wireless Settings menu – WPA-PSK

Enter the appropriate parameters for the type of security from this menu. For PSK authentication using WPA or WPA2, enter the following:

- **Cypher Type:** Choose TKIP, AES or TKIP/AES.
- **Key Type:** Choose ASCII or Hexidecimal.
- **Passphrase:** The password or character string used for wireless station authentication.
- **Key Renewal:** The time (in seconds) after which the Shared Key is changed automatically.

WAN Configuration

To configure the router's WAN configuration settings without running the Setup Wizard, you can access the windows used to configure WAN, LAN, DHCP, and DNS settings directly from the **Home** directory. To access the WAN Settings window, click on the **WAN** menu link on the left side of the first window that appears when you successfully access the web manager.

Select Internet Connection Type

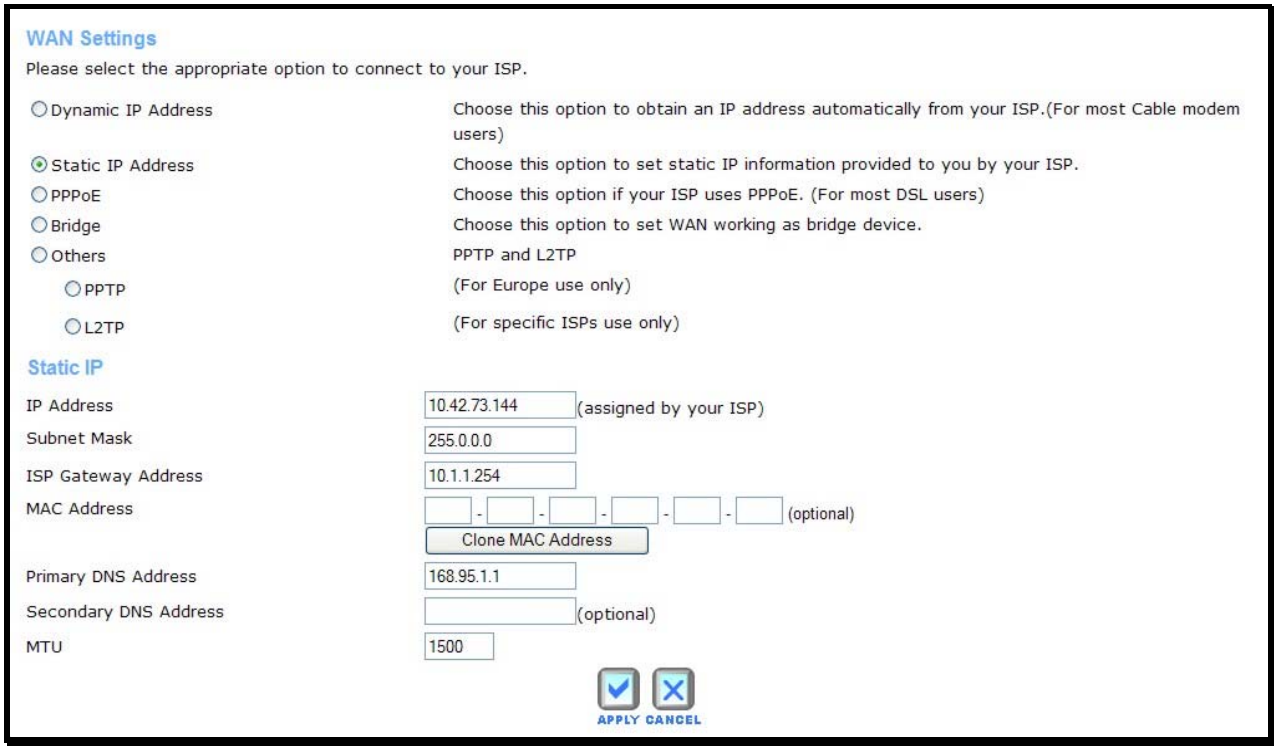
The default Internet Connection menu displays the Dynamic IP (DHCP) Internet Connection Type menu. To select another connection type, use the pull-down **My Internet Connection is:** menu to select the connection type you wish to configure. The menu configuration parameters in the display will change according to the connection option you choose. The available Internet connection types are:

- Static IP Address
- Dynamic IP Address (DHCP)
- PPPoE (Username / Password)
- Bridge Connection
- PPTP (Username / Password)
- L2TP (Username / Password)

Each connection type is discussed in its own section below.

Static IP Address Connection

When the router is configured to use Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask and Gateway IP Address used for the WAN connection.



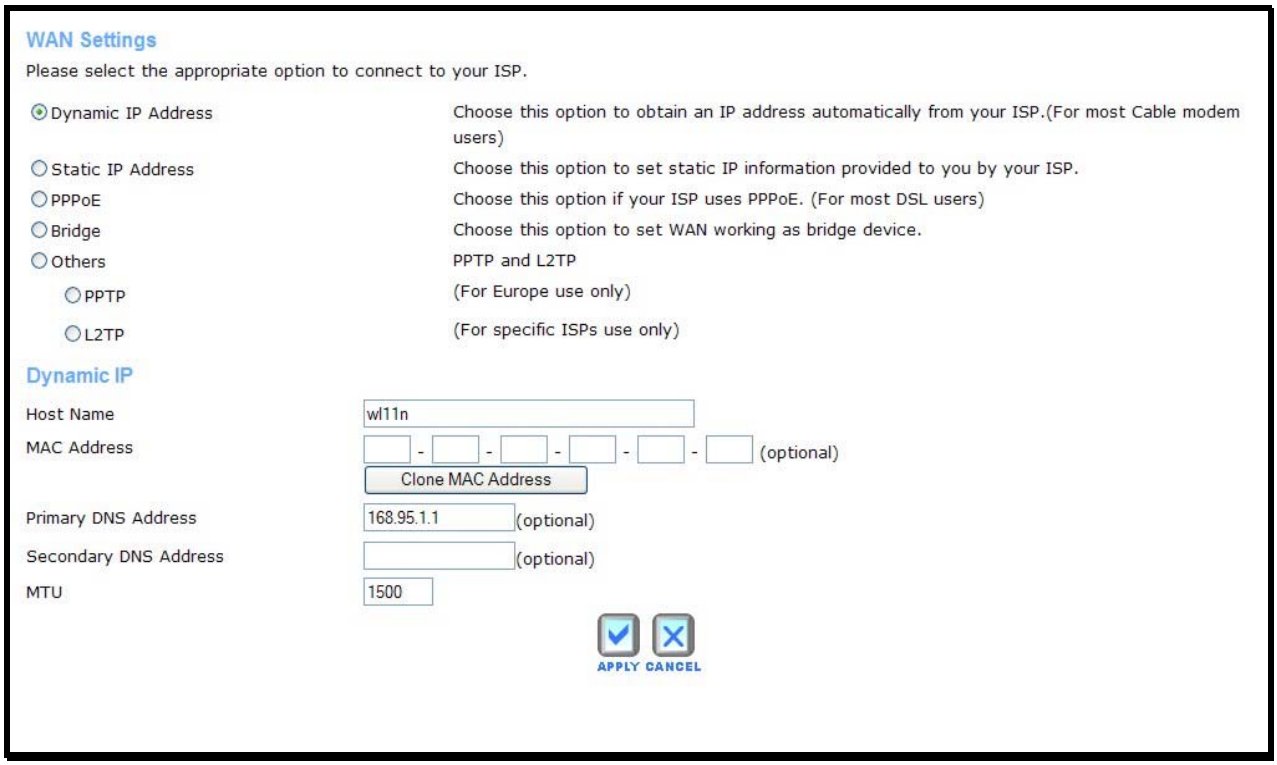
WAN Settings menu - Static IP Address

Configure the Static IP address connection and click the **Apply** button to put the new settings into effect. See the table below for a description of the parameters configured for the connection.

Static IP Parameters	Description
IP Address	This is the permanent global IP address for your account. This is the address that is visible outside your private network. Get this from your ISP.
Subnet Mask	This is the Subnet mask for the WAN interface. Get this from your ISP.
ISP Gateway Address	This is the IP address of your ISP's Gateway router. It provides the connection to the router for IP routed traffic that is outside your ISP's network. That is, this will be the primary connection from the router to most of the Internet. Get this IP address from your ISP.
MAC Address/Clone MAC Address	This field will instruct the user to enter the Media Access Control (MAC) address of the Ethernet Card of your computer, if instructed to do so by your ISP. To quickly accomplish this, click the **Clone MAC Address** button, which will automatically copy the MAC address of your Ethernet card and enter it into the space provided, which will replace the MAC address of the router.
DNS (Primary/ Secondary)	These are the IP addresses of your primary and backup domain name server, which should also be provided to you by your ISP. The router will first try the **Primary DNS Address** to resolve a website's URL IP address. If this IP address fails, the router will then try the **Secondary DNS Address**.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1492 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic throughput.

Dynamic IP Connection

A Dynamic IP Address connection configures the router to automatically obtain its global IP address from a DHCP server on the ISP's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the router requests an IP address.



WAN Settings window – Dynamic IP Address

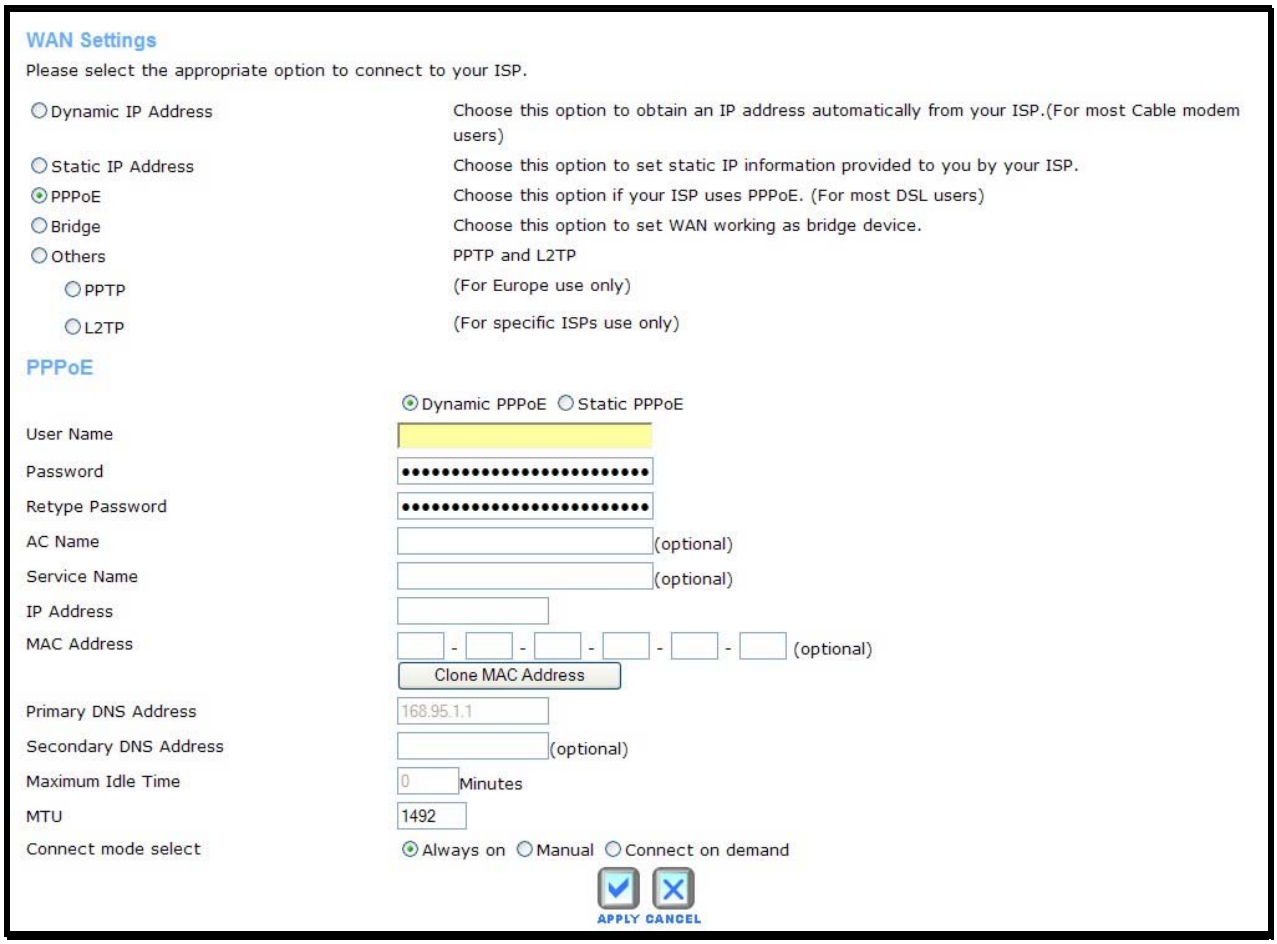
Configure the Dynamic IP address connection and click the **Apply** button to put the new settings into effect. See the table below for a description of the parameters configured for the connection.

Dynamic IP Parameters	Description
Host Name	Enter the Host Name provided if necessary (optional).
MAC Address/Clone MAC Address	This field will instruct the user to enter the Media Access Control (MAC) address of the Ethernet Card of your computer, if instructed to do so by your ISP. To quickly accomplish this, click the **Clone MAC Address** button, which will automatically copy the MAC address of your Ethernet card and enter it into the space provided, which will replace the MAC address of the router.
DNS (Primary/ Secondary)	These are the IP addresses of your primary and backup domain name server, which should also be provided to you by your ISP. The router will first try the **Primary DNS Address** to resolve a website's URL IP address. If this IP address fails, the router will then try the **Secondary DNS Address**.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1492 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic throughput.

PPPoE Connection

PPP or Point-to-Point protocol is a standard method of establishing a network connection/session between networked devices. PPPoE (PPP over Ethernet), as described in RFC 2516, is a method of using PPP through the Ethernet network.

There are two ways to configure the PPoE connection on the router, one is for a **Dynamic PPPoE** configuration, which means the router will implement some settings automatically through DHCP, such as the router's IP address and the default gateway. The other is through a **Static PPPoE** connection, in which the user must configure the IP address and the DNS addresses automatically.



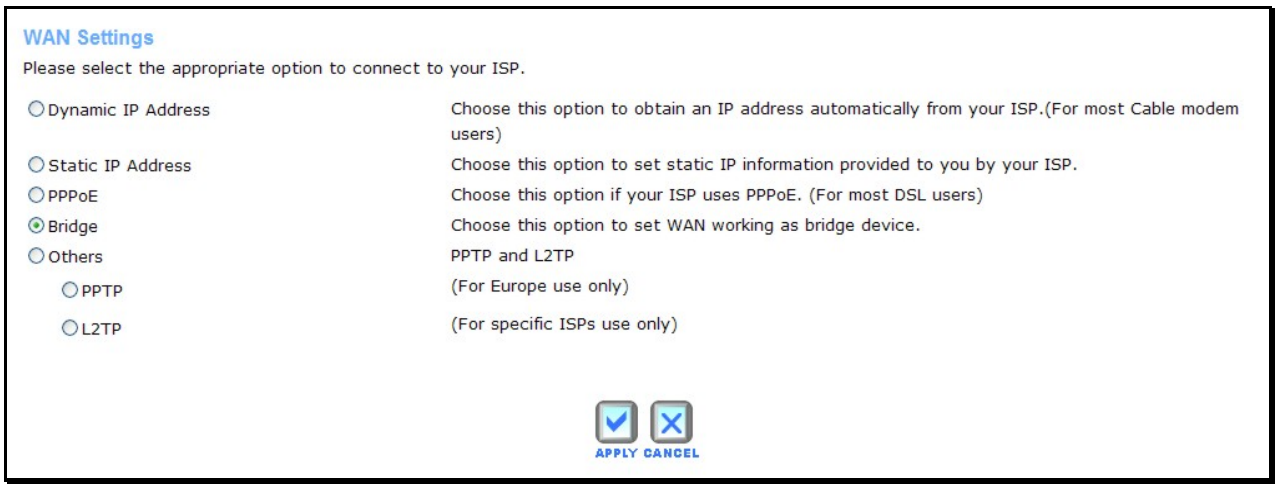
WAN Settings menu – PPPoE connection

Configure the PPPoE connection and click the **Apply** button to put the new settings into effect. See the table below for a description of the parameters configured for the connection.

PPPoE Parameters	Description
User Name	The user name supplied to you by your ISP.
Password	The password supplied to you by your ISP.
Retype Password	Retype the password entered in the **Password** feld.
Service Name	Enter the service name supplied to you by your ISP, if required.
IP Address	Enter the IP address given to you by your ISP. This field is only to be completed if the **Static PPPoE** button is selected.
MAC Address	This field requires the user to enter the Media Access Control (MAC) address of the Ethernet Card of your computer, if instructed to do so by your ISP. To quickly accomplish this, click the **Clone MAC Address** button, which will automatically copy the MAC address of your Ethernet card and enter it into the space provided, which will replace the MAC address of the router.
Primary DNS Address	This entry is for the IP address of your primary domain name server, which should also be provided to you by your ISP. The router will first try the Primary DNS Address to resolve a website's URL IP address. If this IP address fails, the router will then try the Secondary DNS Address. This field is only to be completed if the **Static PPPoE** button is selected.
Secondary DNS Address	The IP address of the secondary domain name server will be used to resolve a website's URL IP address if the **Primary DNS Address** fails. The information in this field should also be provided by your ISP and is only to be completed if the **Static PPPoE** button is selected.
Maximum Idle Time	A value of 0 means that the PPP connection will remain connected. If your network account is billed according to the amount of time the router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the router after the WAN connection has been idle for the amount of time specified. The default value = 5.
MTU	This field refers to the Maximum Transfer Unit, which is the maximum size of a packet, in bytes, that will be accepted by the router. The default setting is 1500 bytes. This field should not be altered unless instructed by your ISP.
Connect Mode Select	This function, with **Connect-on-demand** selected, will allow the router to connect any workstation on your LAN to the Internet upon request. If this function is set at **Always-on**, no request from the workstation will be needed to connect to the Internet. If **Manual** is selected, it will be necessary for the workstation on the LAN to manually connect to the Internet through this router.

Bridge Connection

A Bridge connection does not require much configuration for the router, however most of the router functions are not available in bridge mode.



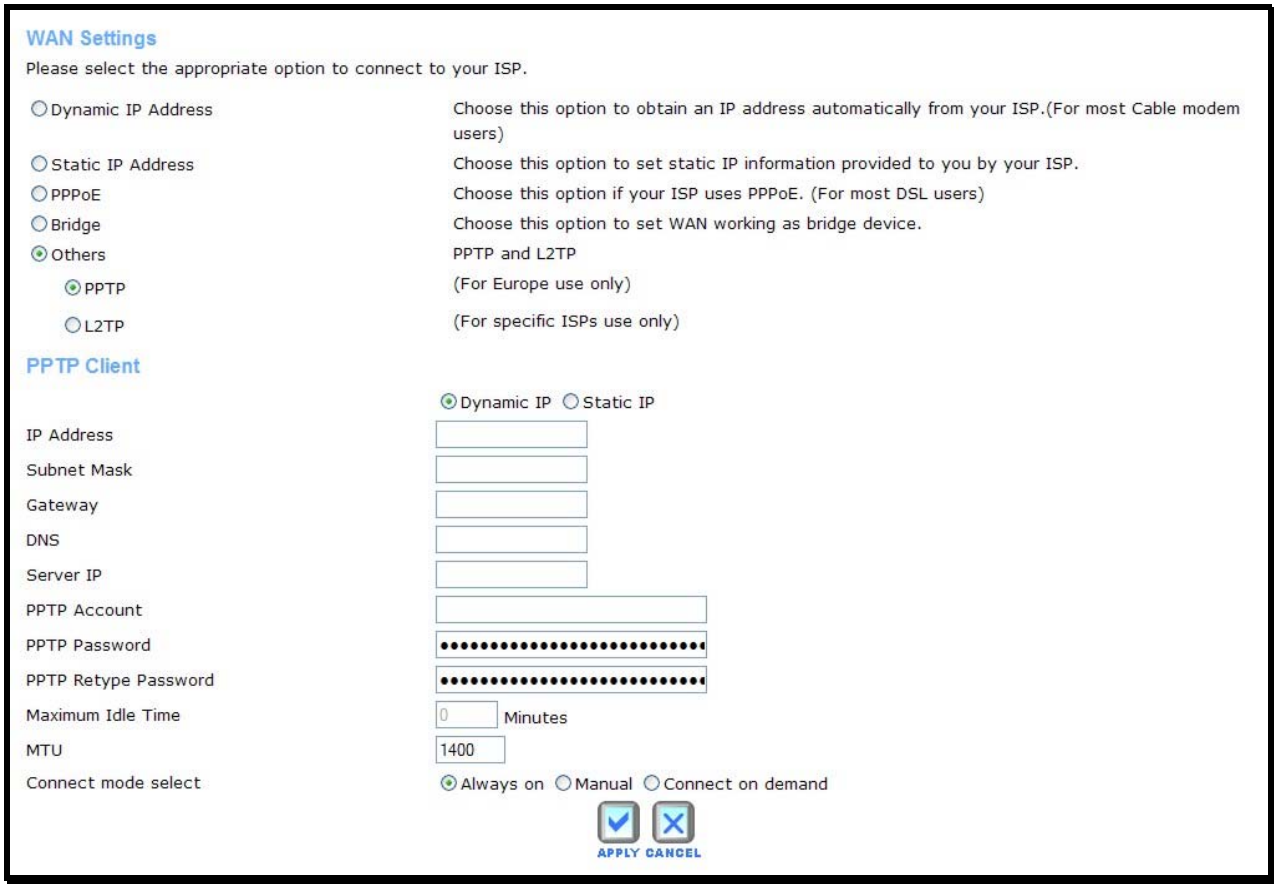
WAN Settings menu – Bridge connection

To configure the Wireless-N Router as a bridge for the WAN connection, select the **Bridge** WAN settings option and click **Apply**. Do this immediately change the IP settings status of the device to DHCP client. Be sure to have a DHCP server running and connected to the network if this option is to be used. Remember that as a bridge, third party connection software is normally required on each computer attempting to get Internet access.

PPTP Connection

If your ISP is using PPTP to provide your Internet connection, the ISP will give you the necessary information to configure the router.

There are two ways to enable the router to become a PPTP client, one is through assigning the router an IP address dynamically, which means that the DHCP protocol will be implemented by the router to automatically configure the IP settings. The user may input the IP settings manually by choosing the Static IP option above the configuring area.



PPTP Internet Connection configuration menu

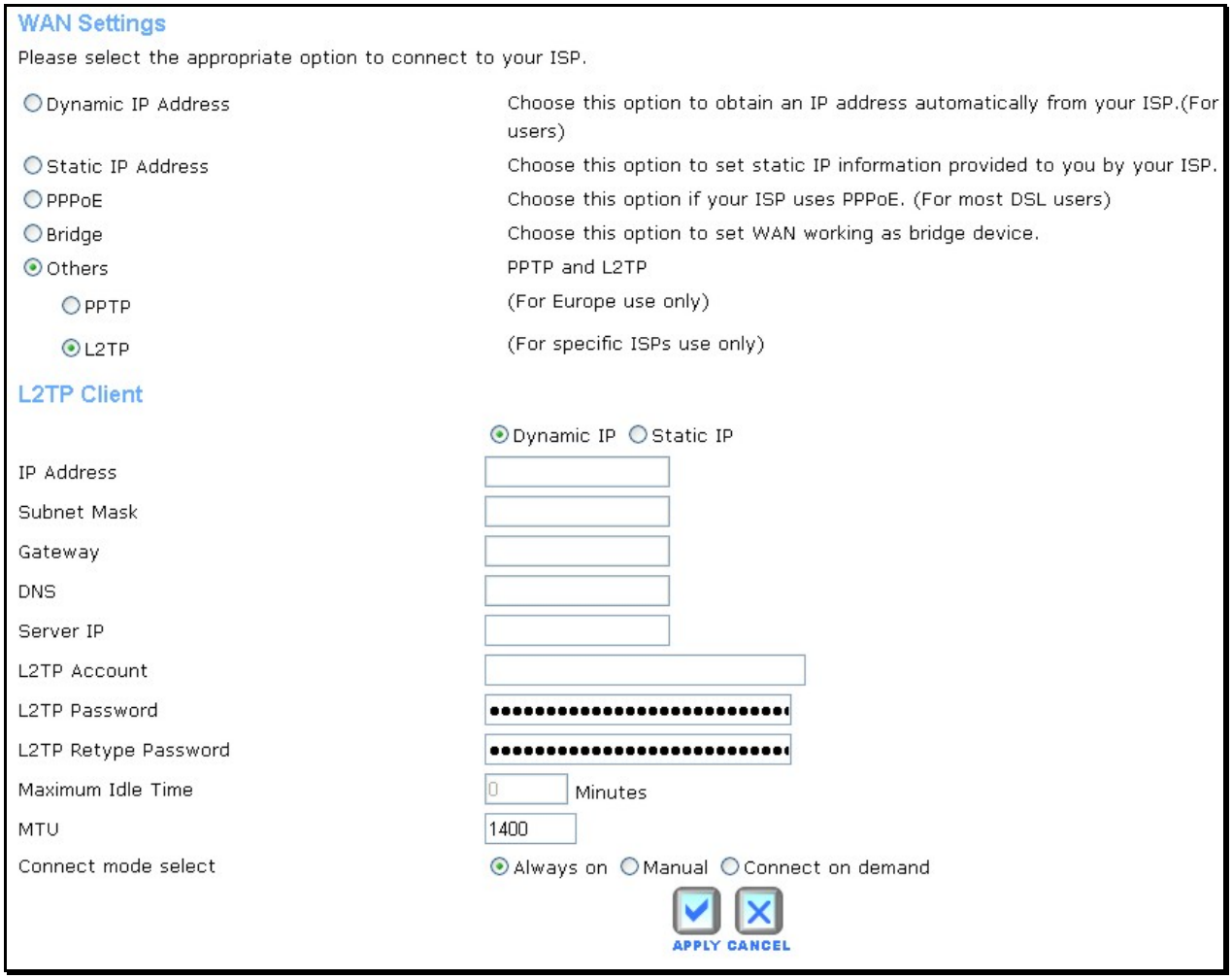
Configure the PPTP connection and click the **Apply** button to put the new settings into effect. See the table below for a description of the parameters configured for the connection.

PPTP Parameters	Description
IP Address	Type the IP address supplied by your ISP.
Subnet Mask	Type the Subnet mask supplied by your ISP.
Gateway	The gateway IP address is used provide access to resources outside your IP Subnet or ISP's network. Type the gateway IP address given to you by your ISP.
DNS	This entry is for the IP address of your primary domain name server, which should also be provided to you by your ISP.
Server IP/Name	Enter the Server IP address for this protocol into this field. This is the IP address of the server computer that will be used, along with your computer, to create the Virtual Private Network. This field must be completed for both the Dynamic IP and Static IP options
PPTP Account	Enter the PPTP account name, provided to you by your ISP, here.
PPTP Password	Enter your password for this PPTP account here, as stated to you by your ISP.
PPTP Confirm Password	Retype the password entered in the **PPTP Password** field.
Maximum Idle Time	A value of 0 in this field means that the PPTP connection will remain connected. If your network account is billed according to the amount of time the router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the router after the WAN connection has been idle for the amount of time specified. The default value = 5.
MTU	This field refers to the Maximum Transfer Unit, which is the maximum size of a packet, in bytes, that will be accepted by the router. The default setting is 1500 bytes. This field should not be altered unless instructed by your ISP.
Connect Mode Select	This function, with **Connect-on-demand** selected, will allow the router to connect any workstation on your LAN to the Internet upon request. If this function is set at **Always-on**, no request from the workstation will be needed to connect to the Internet. If **Manual** is selected, it will be necessary for the workstation on the LAN to manually connect to the Internet through this router.

L2TP Connection

If your ISP is using L2TP to provide your Internet connection, the ISP will give you the necessary information to configure the router.

There are two ways to enable the router to become a L2TP client, one is through assigning the router an IP address dynamically, which means that the DHCP protocol will be implemented by the router to automatically configure the IP settings. The user may input the IP settings manually by choosing the Static IP option above the configuring area.



L2TP Internet Connection configuration menu

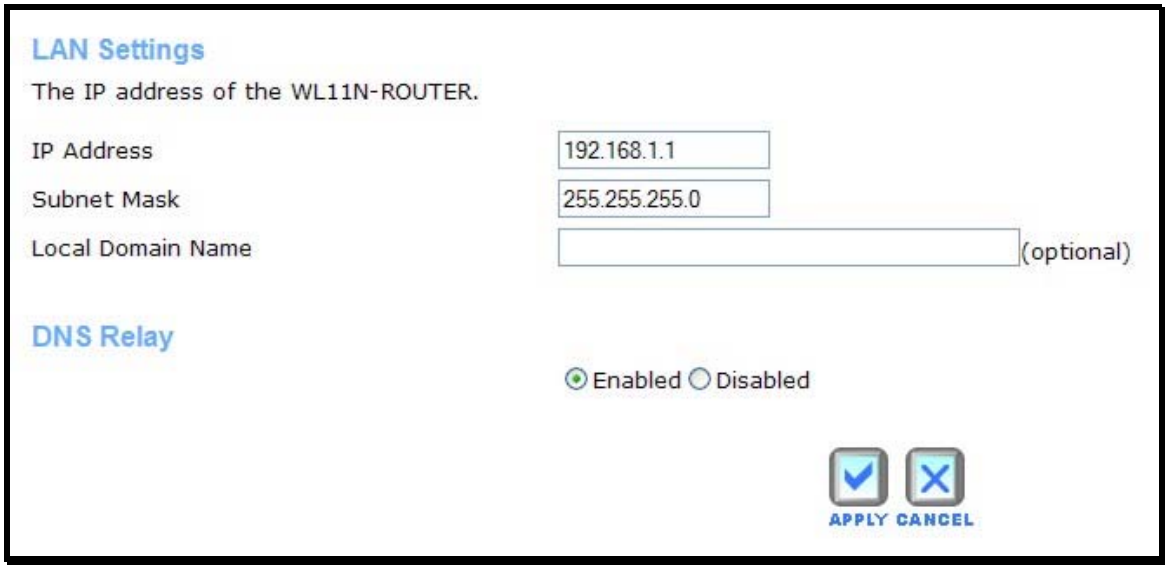
Configure the L2TP connection and click the **Apply** button to put the new settings into effect. See the table below for a description of the parameters configured for the connection.

L2tP Parameters	Description
IP Address	Type the IP address supplied by your ISP.
Subnet Mask	Type the Subnet mask supplied by your ISP.
Gateway	The gateway IP address is used provide access to resources outside your IP Subnet or ISP's network. Type the gateway IP address given to you by your ISP.
DNS	This entry is for the IP address of your primary domain name server, which should also be provided to you by your ISP.
Server IP/Name	Enter the Server IP address for this protocol into this field. This is the IP address of the server computer that will be used, along with your computer, to create the Virtual Private Network. This field must be completed for both the Dynamic IP and Static IP options
L2TP Account	Enter the L2TP account name, provided to you by your ISP, here.
L2TP Password	Enter your password for this L2TP account here, as stated to you by your ISP.
L2TP Confirm Password	Retype the password entered in the **L2TP Password** field.
Maximum Idle Time	A value of 0 in this field means that the L2TP connection will remain connected. If your network account is billed according to the amount of time the router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the router after the WAN connection has been idle for the amount of time specified. The default value = 5.
MTU	This field refers to the Maximum Transfer Unit, which is the maximum size of a packet, in bytes, that will be accepted by the router. The default setting is 1500 bytes. This field should not be altered unless instructed by your ISP.
Connect Mode Select	This function, with **Connect-on-demand** selected, will allow the router to connect any workstation on your LAN to the Internet upon request. If this function is set at **Always-on**, no request from the workstation will be needed to connect to the Internet. If **Manual** is selected, it will be necessary for the workstation on the LAN to manually connect to the Internet through this router.

LAN

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the router is the base address used for DHCP. In order to use the router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the router. See the next section for information on DHCP setup.

To access the **LAN IP** menu, click the **LAN** link in the **Home** directory.



LAN Settings – Router IP address menu

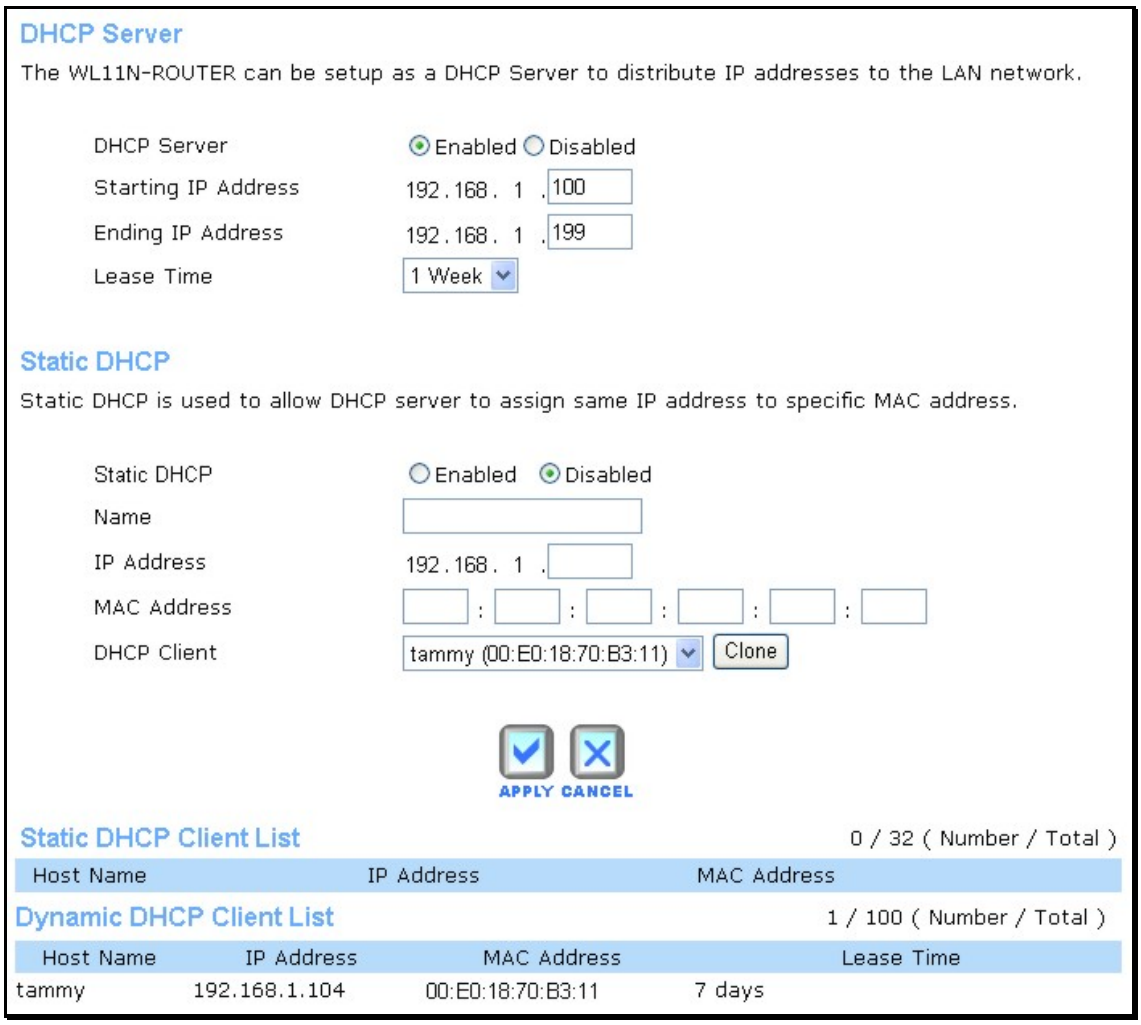
To change the LAN **IP Address** or **Subnet Mask**, type in the desired values and click the **Apply** button. Your web browser should automatically be redirected to the new IP address. You will asked to login again to the router's web manager.

This IP address is private to your internal network and cannot be seen on the Internet. The default **IP Address** is 192.168.1.1 and the **Subnet Mask** is 255.255.255.0.

In addition, the router can be configured to relay DNS from your ISP or another available service to workstations on your LAN. When **DNS Relay** is ***Enabled***, the router will accept DNS requests from hosts on the LAN and forward them to the ISP (or alternative) DNS servers. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most users who are using the router for DHCP service on the LAN and are using DNS servers on the ISP's network, will leave DNS relay enabled.

DHCP

The DHCP server is enabled by default for the router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the router though the Ethernet port. When the router is used for DHCP it becomes the default gateway for DHCP client connected to it. The IP address pool can be up to 253 IP addresses and must be in the subnet of the router's IP address. The default IP address pool uses 100 IP addresses in the 192.168.1.100 – 192.168.1.199 range.



DHCP Server for LAN Settings menu

To display the **DHCP Server** menu, click the **DHCP** link in the **Home** directory. Any active DHCP clients appear in the DHCP Clients List with their IP address and MAC address listed.

The options for DHCP service are as follows:

- Use the router as a DHCP server for your LAN. (DHCP Server *Enabled*)
- Disable DHCP service and manually configure IP settings for workstations.
- Select Static IP Addresses in the subnet for specified devices that do not age out - this can be used in combination with normal DHCP service.

Use the Router for DHCP

To use the built-in DHCP server, click to select the **DHCP Server** *Enabled* option if it is not already selected. The IP Address Pool settings can be adjusted. The **Start IP** address is the lowest available IP address (default = 192.168.1.100). If you change the IP address of the router this will change automatically to be 1 more that the IP address of the router.

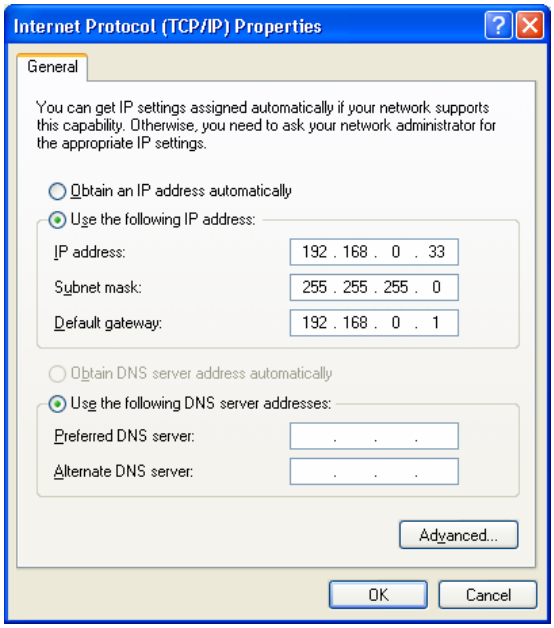
The **End IP** address is the highest IP address number in the pool. Type in the **Lease Time** in the entry field provided. This is the amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

Disable the DHCP Server

To disable DHCP, click to select the *Disabled* option and click on the **Apply** button. Choosing this option requires that workstations on the local network must be configured manually or use another DHCP server to obtain IP settings.

If you configure IP settings manually, make sure to use IP addresses in the subnet of the router. You will need to use the router's IP address as the Default Gateway for the workstation in order to provide Internet access.

NOTE: To manually configure IP settings on Windows workstations, open the TCP/IP Properties menu and select the "Use the following IP address" option. You will need to supply the computer IP address, Subnet mask and Default gateway (usually the IP address of router).



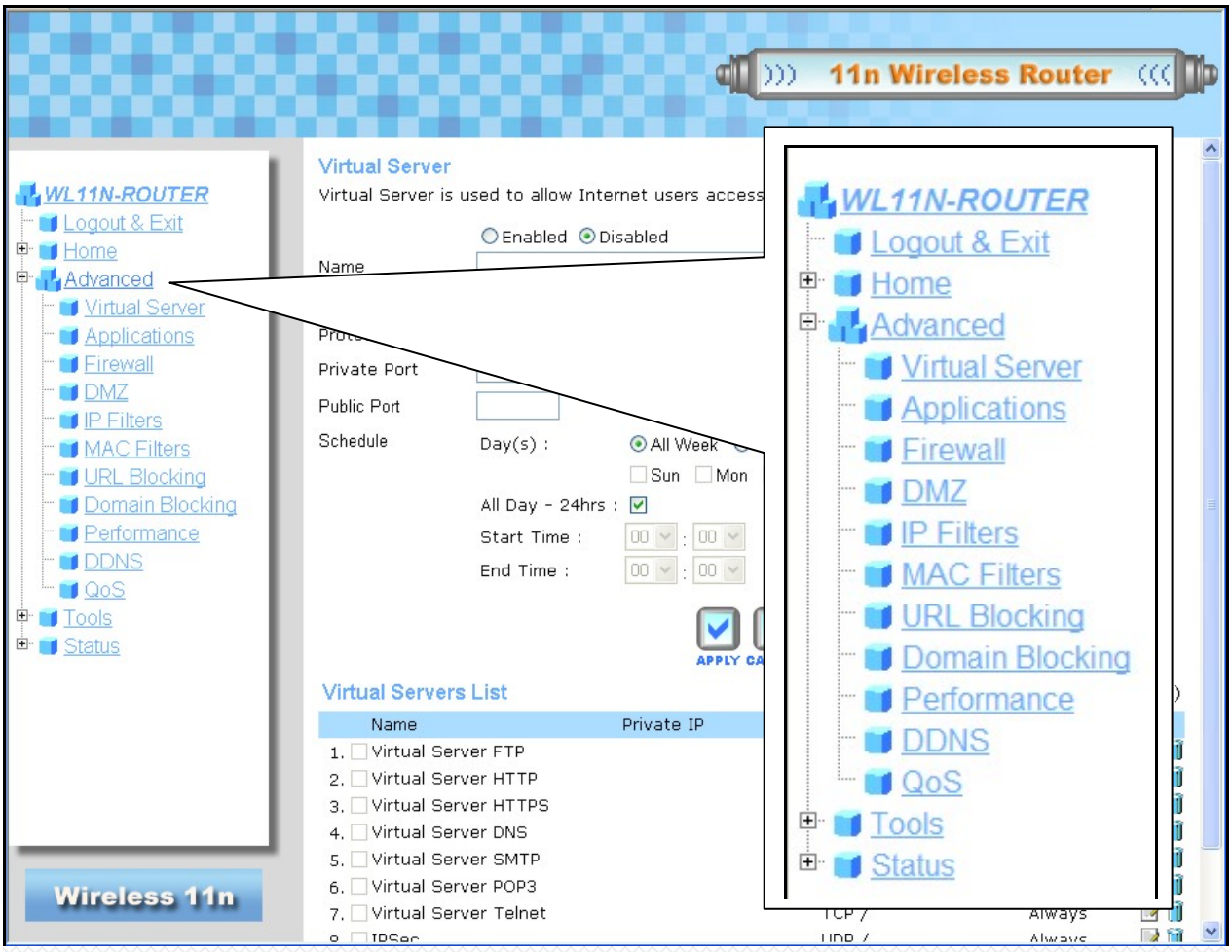
Static IP Address with DHCP

If the router has the DHCP server enabled it is possible to permanently assign IP addresses to workstations specified by their MAC address. Up to five IP addresses may be assigned to five different devices. This will take the chosen IP address used out of the available addresses in the dynamic IP address pool and give a permanent lease time for the IP address to the selected device.

To assign an IP address that will not age out, type in the **MAC Address** of the device and its static **IP Address** in the spaces provided. Use the format: 00-00-00-00-00-00 for the MAC address and the standard format: 192.168.1.xxx for the IP address. A Static DHCP Client List will appear below the DHCP Client list with any clients that have been configured for static IP address assignment.

Advanced Directory Menus

This section introduces and describes the management features that have not been presented in the previous chapter. These include the more advanced features used for network management and security as well as administrative tools to manage the router, view statistics and other information used to examine performance and for troubleshooting.

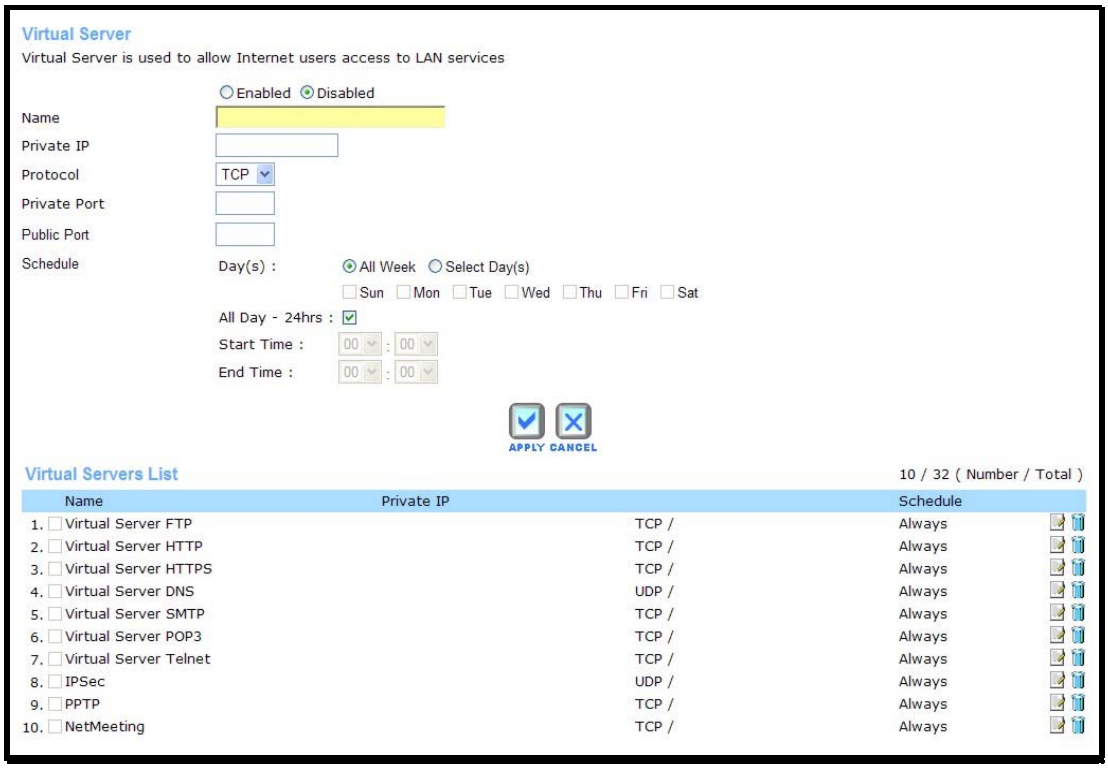


Advanced Directory menus

Use your mouse to click the parent directory links and menu links in order to display the various configuration and read-only windows discussed below.

Virtual Server

Use the **Virtual Server** menu to set up static port forwarding rules applied to inbound (WAN-to-LAN) traffic. The Virtual Server function allows remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The router will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the LAN IP address you specify. Remember that the specified Private IP Address must be within the useable range of the subnet occupied by the router. Port redirection can also be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the router to direct HTTP packets to a designated HTTP server in the DMZ.



Virtual Server menu

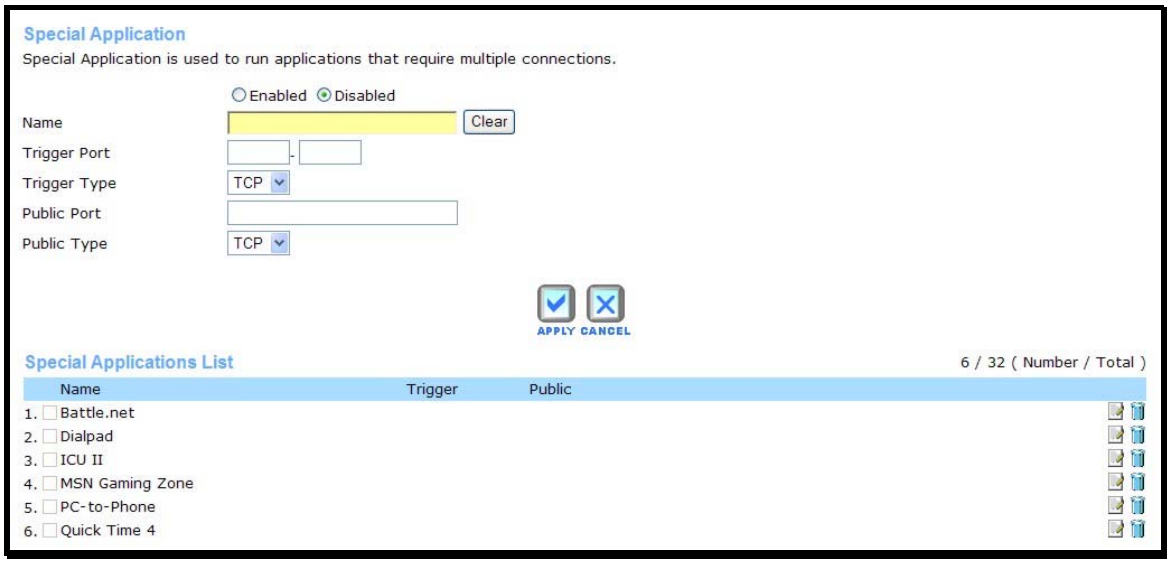
To configure a new port-forwarding rule, follow these steps:

1. Click on the Enabled option for **Virtual Server**.
2. Type a **Name** for the rule being created.
3. Type the **Private IP** address of the server or station on the LAN used for the rule.
4. Select the **Protocol** used for the rule, TCP, UDP or Both.
5. Type the **Private Port** number used for the redirection and **Public Port** number normally used for the service.
6. Choose an available **Schedule** for the rule to be applied. Schedules can be created using the **Schedule** menu in the **Tools** directory.
7. Click the **Apply** button to put the rule into effect. The newly created forwarding rule appears listed in the **Virtual Server List**.

To modify an existing rule, click on the notepad icon in the last column of the Virtual Server List. To remove a rule, click the **X** to delete it.

Applications

Use the **Applications** menu to set up triggered port forwarding rules applied to inbound (WAN-to-LAN) traffic. Triggered ports are used for applications that require multiple ports. Examples of multiple port applications are peer-to-peer file sharing, instant messaging or video conferencing.



Applications menu

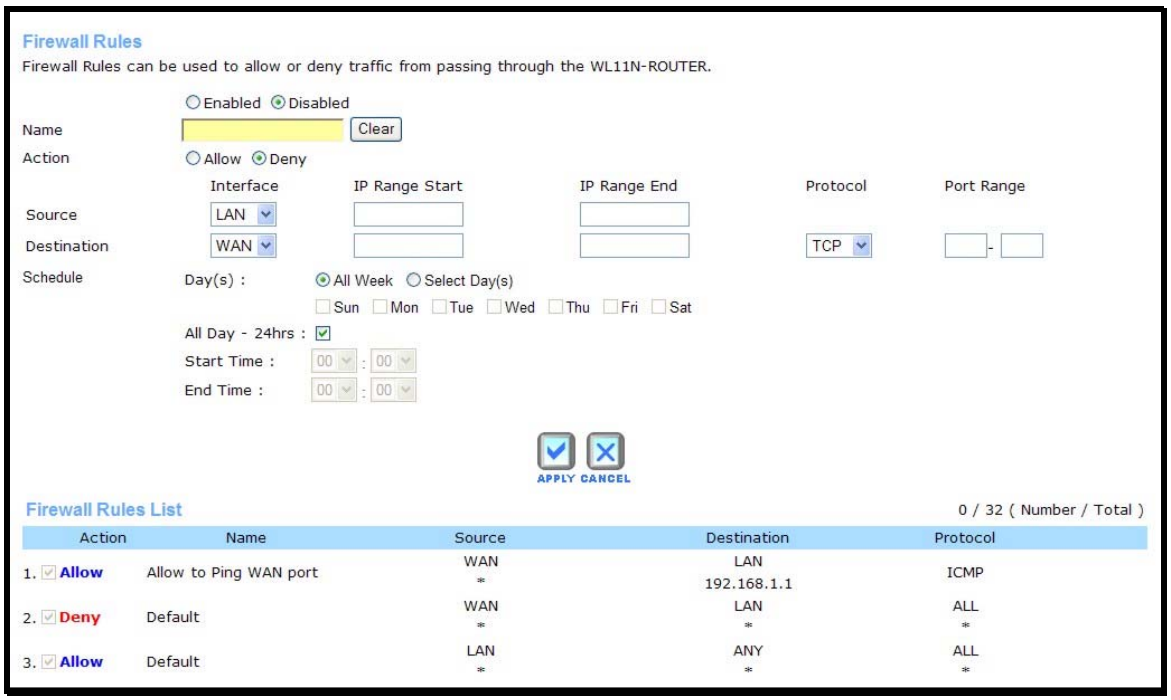
To configure a new application triggered port forwarding rule, follow these steps:

1. Click on the Enabled option for **Special Application**.
2. Type a **Name** for the rule being created.
3. Type the **Trigger Port** or port range used for the rule.
4. Select the **Trigger Type** used for the rule, TCP, UDP or Both.
5. Type the **Public Port** number normally used for the application.
6. Select the **Public Type** used for the rule, TCP, UDP or Both.
7. Choose an available **Schedule** for the rule to be applied. Schedules can be created using the **Schedule** menu in the **Tools** directory.
8. Click the **Apply** button to put the rule into effect. The newly created forwarding rule appears listed in the **Special Applications List**.

To modify an existing rule, click on the notepad icon in the last column of the Special Applications List. To remove a rule, click the **X** to delete it.

Firewall

Firewall rules in the router are put in place to allow or block specified traffic. The rules are based on IP address and TCP/UDP port.



Firewall menu

Configure the filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the Firewall Rule List.

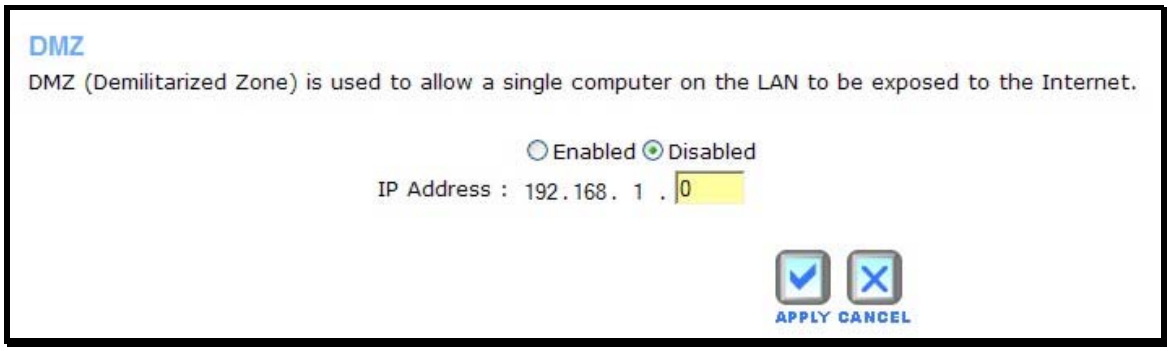
To configure a new application triggered port forwarding rule, follow these steps:

1. Click on the Enabled option for **Firewall Rules**.
2. Type a **Name** for the rule being created.
3. Choose the **Action** to be applied, Allow or Deny (block) the traffic to pass through.
4. For the **Source** interface of the traffic, choose LAN, WAN or Any and type an IP address range to which to action specified in the rule.
5. For the **Destination** interface of the traffic, choose LAN, WAN or Any and type an IP address range to which to action specified in the rule. There is an option to specify the protocol, Any, TCP, UDP or ICMP. For TCP and UDP traffic, a port or port range must be specified.
6. Choose an available **Schedule** for the rule to be applied. Schedules can be created using the **Schedule** menu in the **Tools** directory.
7. Click the **Apply** button to put the rule into effect. The newly created forwarding rule appears listed in the **Firewall Rules List**.

To modify an existing rule, click on the notepad icon in the last column of the Firewall Rules List. To remove a rule, click the **X** to delete it.

DMZ

Since some applications are not compatible with NAT, the router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.

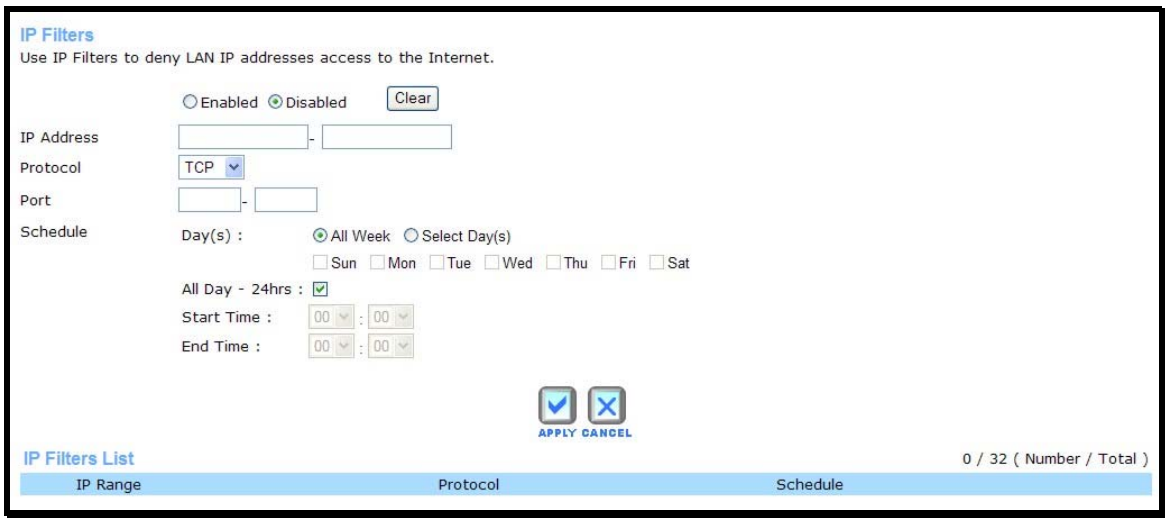


DMZ menu

To designate a DMZ IP address, select the Enabled radio button, type in the **IP Address** of the server or device on your LAN, and click the **Apply** button. To remove DMZ status from the designated IP address, select the Disabled radio button and click Apply. It will be necessary to save the settings and reboot the router before the DMZ is activated.

IP Filters

This menu allows the user to allow or deny LAN IP addresses access to the Internet. Rules are based on IP address and TCP/UDP port.



IP Filters menu

Configure the filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the IP Filters List.

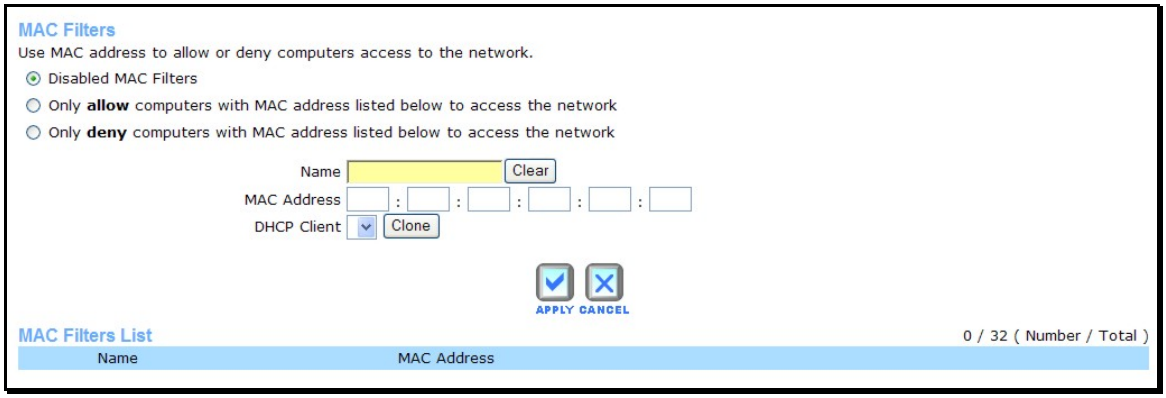
To configure a new MAC Filter rule, follow these steps:

1. Click on the Enabled option for **IP Filters**.
2. Type a **Name** for the rule being created.
3. Type the **IP Range** of address to which the rule applies.
4. (Optional) Select the **Protocol** used for the rule, TCP, UDP or Both, and type the **Port** or port range to which the rule is applied.
5. Choose an available **Schedule** for the rule to be applied. Schedules can be created using the **Schedule** menu in the **Tools** directory.
6. Click the **Apply** button to put the rule into effect. The newly created IP filter rule appears listed in the **IP Filters List**.

To modify an existing rule, click on the notepad icon in the last column of the Firewall Rules List. To remove a rule, click the **X** to delete it.

MAC Filters

MAC filters are used to block or allow network access. This is a common method of restricting access to wireless networks and can be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address.



MAC Filters menu

Configure the MAC filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the **MAC Filters List**.

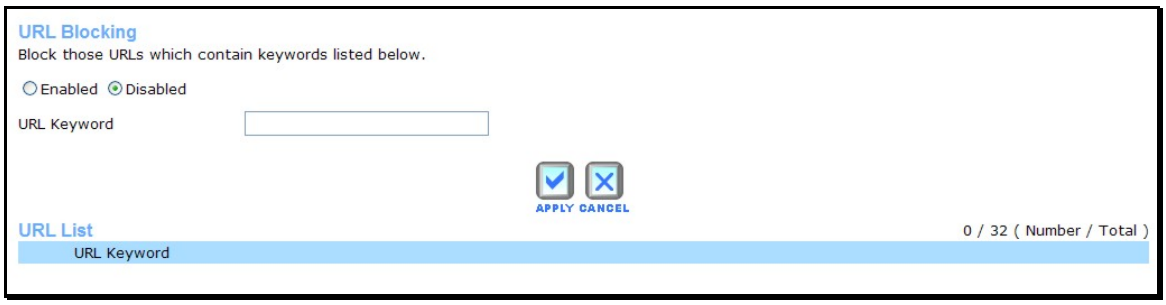
To configure a new IP Filter rule, follow these steps:

1. Click on the option for **Set MAC Filters** to allow or deny access to the MAC filters on the list.
2. Type a **Name** for the rule being created.
3. Type the **MAC Address** to which the rule applies or select an active client from the **DHCP Client** pull-down menu and click on the **Clone** button to select that client, the MAC address will appear.
4. Choose an available **Schedule** for the rule to be applied. Schedules can be created using the **Schedule** menu in the **Tools** directory.
5. Click the **Apply** button to put the rule into effect. The newly created MAC filter rule appears listed in the **MAC Filters List**.

To modify an existing rule, click on the notepad icon in the last column of the MAC Rules List. To remove a rule, click the **X** to delete it.

URL Blocking

URL blocks are used to block or allow access to specific websites. Enter the URLs in the **URL Keyword** field and click the **Apply** button to add the URL to the URL Blocking List.



URL Blocking menu

Configure the URL blocking rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the **URL Blocking List**.

To configure a new URL blocking rule, follow these steps:

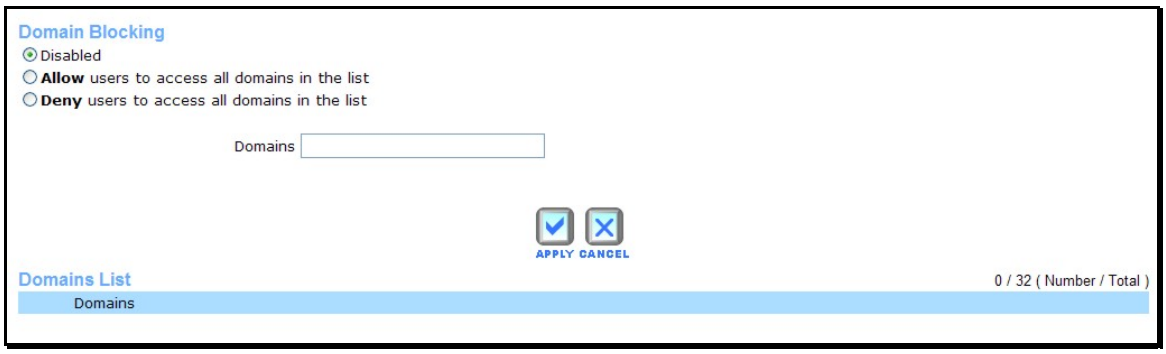
1. Click on the option for **Set URL Blocking Action** to allow or deny access to the URL being added to the list.
2. Type a **Name** for the rule being created.
3. Type the **URL Keyword** to which the filter is applied.
4. Choose an available **Schedule** for the rule to be applied. Schedules can be created using the **Schedule** menu in the **Tools** directory.
5. Click the **Apply** button to put the rule into effect. The newly created URL blocking rule appears listed in the **URL Blocking List**.

To modify an existing rule, click on the notepad icon in the last column of the URL Blocking List. To remove a rule, click the **X** to delete it.

NOTE: The URL keyword blocking is applied to all forms of the word whether or not it appears separated in the URL. For example, blocking any URL with the word “sex” would block a URL with “sex” as part of it, so websites with “essex” or “sextant” in the URL would be blocked.

Domain Blocking

Domain blocks are used to block or allow access to specific domains including all web pages contained in the domain.



Domain Blocking menu

Configure the Domain blocking rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the **Domain Blocking List**.

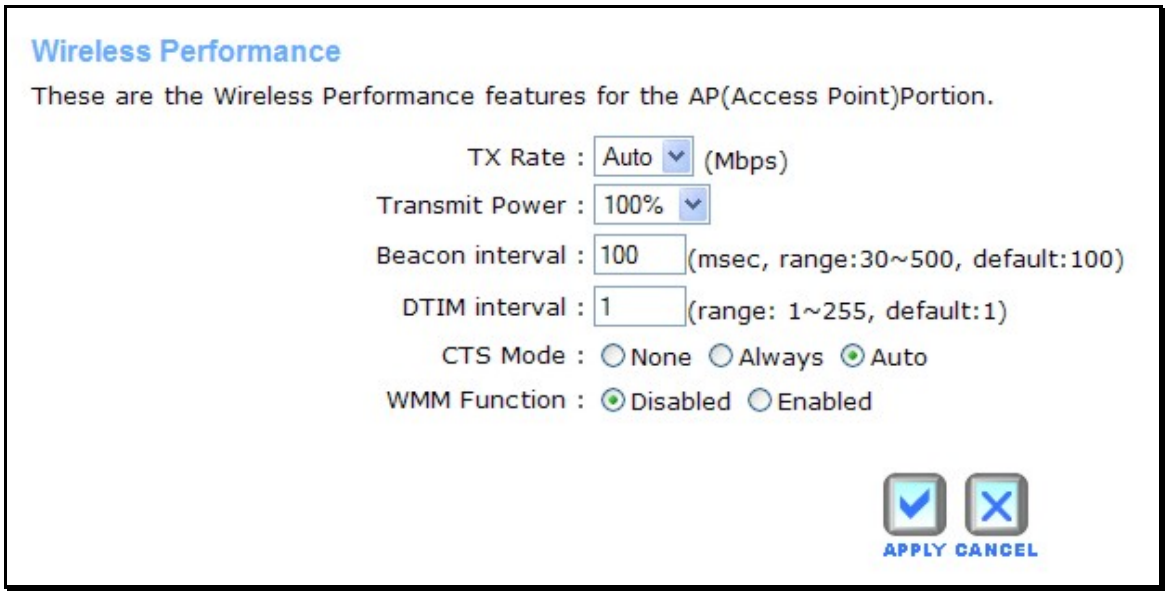
To configure a new Domain blocking rule, follow these steps:

1. Click on the option for **Set Domain Blocking Action** to allow or deny access to the Domain being added to the list.
2. Type a **Name** for the rule being created.
3. Type the **Domain** to which the filter is applied.
4. Choose an available **Schedule** for the rule to be applied. Schedules can be created using the **Schedule** menu in the **Tools** directory.
5. Click the **Apply** button to put the rule into effect. The newly created domain blocking rule appears listed in the **Domain Blocking List**.

To modify an existing rule, click on the notepad icon in the last column of the Domain Blocking List. To remove a rule, click the **X** to delete it.

Wireless Performance

The **Wireless Performance** menu is used to configure settings for the Wireless Broadband Router's access point. Configuring these settings may improve the performance but if you are not familiar with them, leave them at the default settings. Click **Apply** when you have completed your changes.



Wireless Performance menu

See the table below for a description of Wireless Performance menu parameters.

Performance Parameter	Description
Tx Rate	A pull-down menu for selecting the transmitting rate: Auto, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54.
Transmit Power	Allows the user to adjust the transmit power of the router. A high transmit power allows a greater area range of accessibility to the router. When multiple overlapping access points are present, it may be desirable to reduce transmission power.
Beacon Interval	Beacons are emitted from the router in order to synchronize the wireless network. You may set the Beacon Interval range between 20-100 microseconds per beacon sent. The default is 100.
DTIM Interval	DTIM (Delivery Traffic Indication Message) Period is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default setting is 3.
CTS Mode	The Clear To Send mode is designed to minimize collisions among wireles devices. Most users will want to keep the default setting of Auto.
WMM Function	Enable or disable the Wireless MultiMedia function.

Dynamic DNS

The Wireless-N Router supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyper linked URL in the form hostname.dyndns.org, Many ISPs assign public IP addresses using DHCP, and this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS providers.

Dynamic DNS Configuration menu

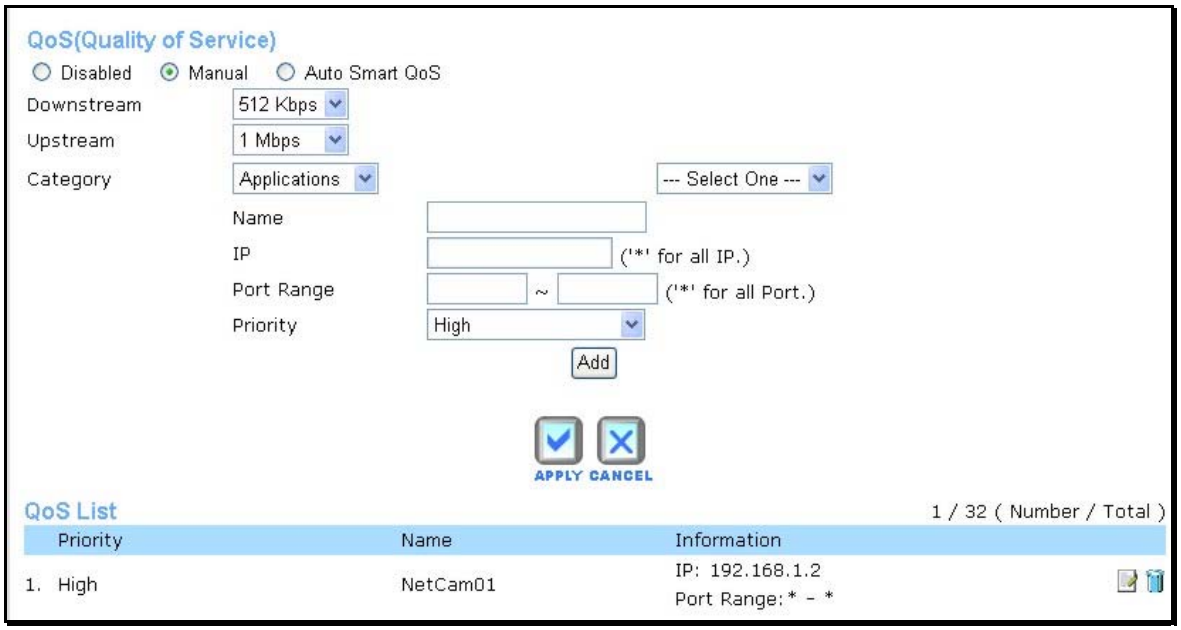
Please note that DDNS requires that an account be setup with one of the supported DDNS servers prior to engaging it on the router. This function will not work without an accepted account with a DDNS server. Enter the required DDNS information and click **Apply** to set this information in the router.

NOTE: DDNS requires that an account be setup with one of the supported DDNS servers prior to engaging it on the router. This function will not work without an accepted account with a DDNS server.

DDNS Parameters	Description
Server Address	Select one of the DDNS registration organizations form those listed in the pull-down menu. Available servers include DynDns.org and No-IP.com.
Host Name	Enter the host name of the DDNS server.
Username	Enter the username given to you by your DDNS server.
Password	Enter the password or key given to you by your DDNS server

QoS

QoS or Quality of Service is used to assign priority for qualified traffic that passes through the Router. The QoS menu includes options for applications that optimizing QoS settings for the ports relevant to common applications such as Skype or online gaming. The QoS menu also allows customized bandwidth settings (upstream/downstream) for specific devices.



QoS menu

QoS is disabled by default. To use QoS, first enable it by selecting the **Manual** or **Auto Smart QoS** option. Choosing the Auto Smart QoS option does not require any additional configuration. It will automatically optimize QoS according to the type of data stream. Choose the Auto Smart QoS option on traffic diverse networks that already support QoS priority in other devices such a managed switches. You might also try the Auto Smart option and test various applications for performance, then if necessary enter QoS settings manually. Use the Manual option if you want to specify bandwidth for a devices or devices on the network. Bandwidth settings can also be configured using the Auto Smart option, the bandwidth settings will be applied globally and not to any specific device (IP address).

To configure a individual IP address for a pre-configured (from the list) application QoS, choose the online game or application first to place the port and priority values in the entry fields, then change the Category to Customized to specify the IP address.

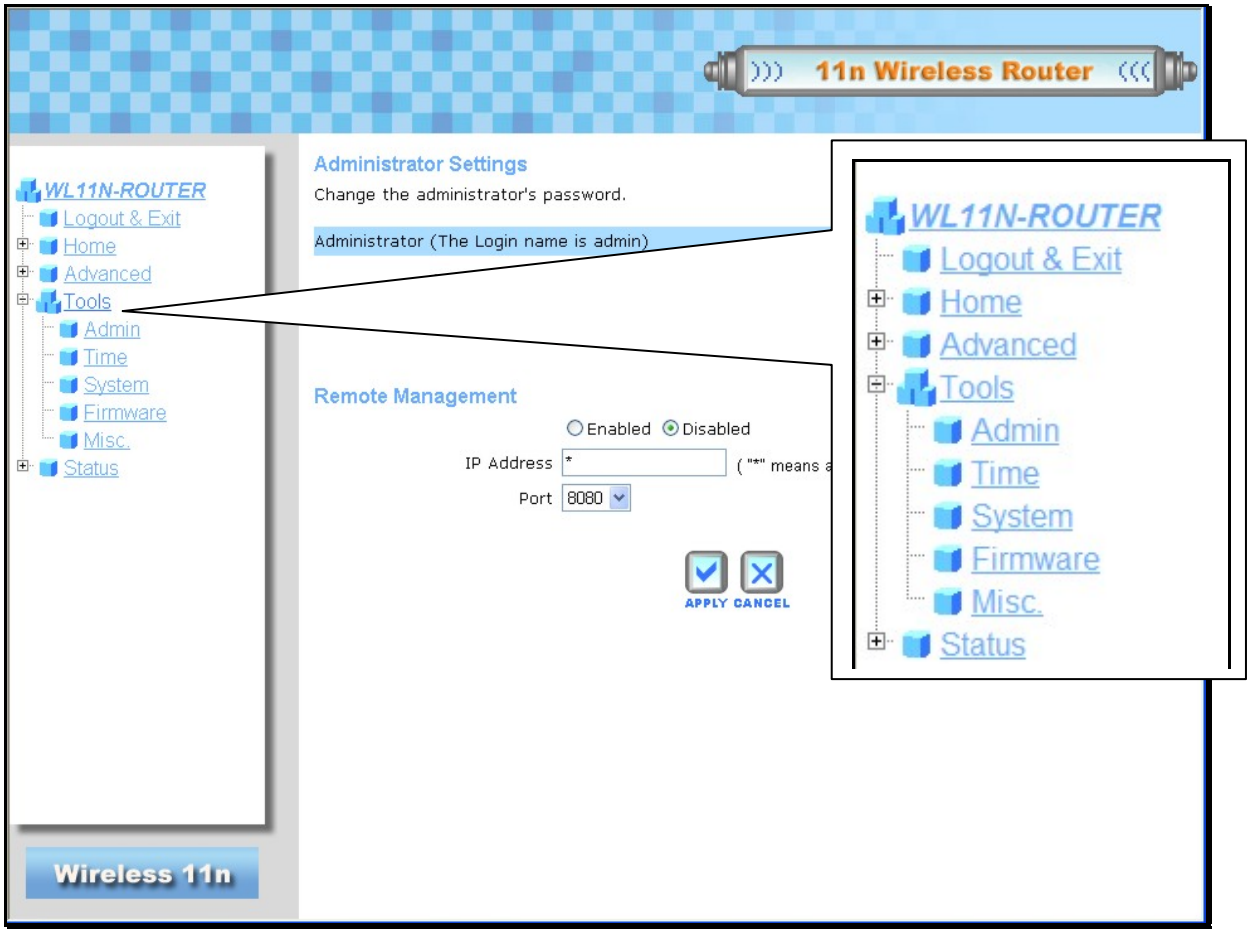
See the table below for a description of the QoS menu parameters.

NOTE: Be aware that changing QoS settings can enhance the performance of specific applications at the expense of other applications. Monitoring network performance is a good idea following changes to QoS settings on networks with high traffic volume or diverse network applications, to determine if the new QoS settings are affecting other applications.

QoS	Description
QoS enable/disable	Disabled by default. To enable QoS, choose the Auto Smart QoS option or the Manual option to specify QoS settings by application or for specified IP addresses.
Downstream	Downstream bandwidth can be configured with a maximum allowed speed ranging from 64 Kbps to 80 Mbps. For Manually configured QoS, the bandwidth restriction applies to the application or IP address being configured. For Auto Smart QoS, the bandwidth restriction is global.
Upstream	Upstream bandwidth can be configured with a maximum allowed speed ranging from 64 Kbps to 80 Mbps. For Manually configured QoS, the bandwidth restriction applies to the application or IP address being configured. For Auto Smart QoS, the bandwidth restriction is global.
Category	For manual QoS configuration, choose **Applications**, **Online Game** or **Customized** options. Applications or online games can then be selected from the drop-down menu. The pre-configured QoS applications include: web browser, MSN Messenger, Skype and Yahoo Message. The online games include: Counter Strike, Half Life, World of Warcraft, Quake I & II and Diablo. You can choose an application first to enter the parameters automatically, then choose the Customized option to specify an IP address.
Name	For Customized QoS configuration enter, the name of the device for which the QoS settings will apply.
IP	For Customized QoS configuration enter, the IP address of the device for which the QoS settings will apply. Enter an asterisk (*) to apply to all IP addresses.
Port	For Customized QoS configuration enter, the port or port range used for the application. Enter an asterisk (*) to apply to all ports.
Priority	Select the QoS priority used for the application being configured. The options in order from lowest priority to highest are Low, Normal, Medium and High.

Tools

Click the **Tools** directory link to reveal the menu links for various functions located in this directory. The **Administrator Settings** window is the first item in the **Tools** directory. This window is used to change the system password used to access the web manager, to save or load router configuration settings and to restore default settings. The functions in this and the other **Tools** menus are described below.



Tools Directory menus

Change System Password

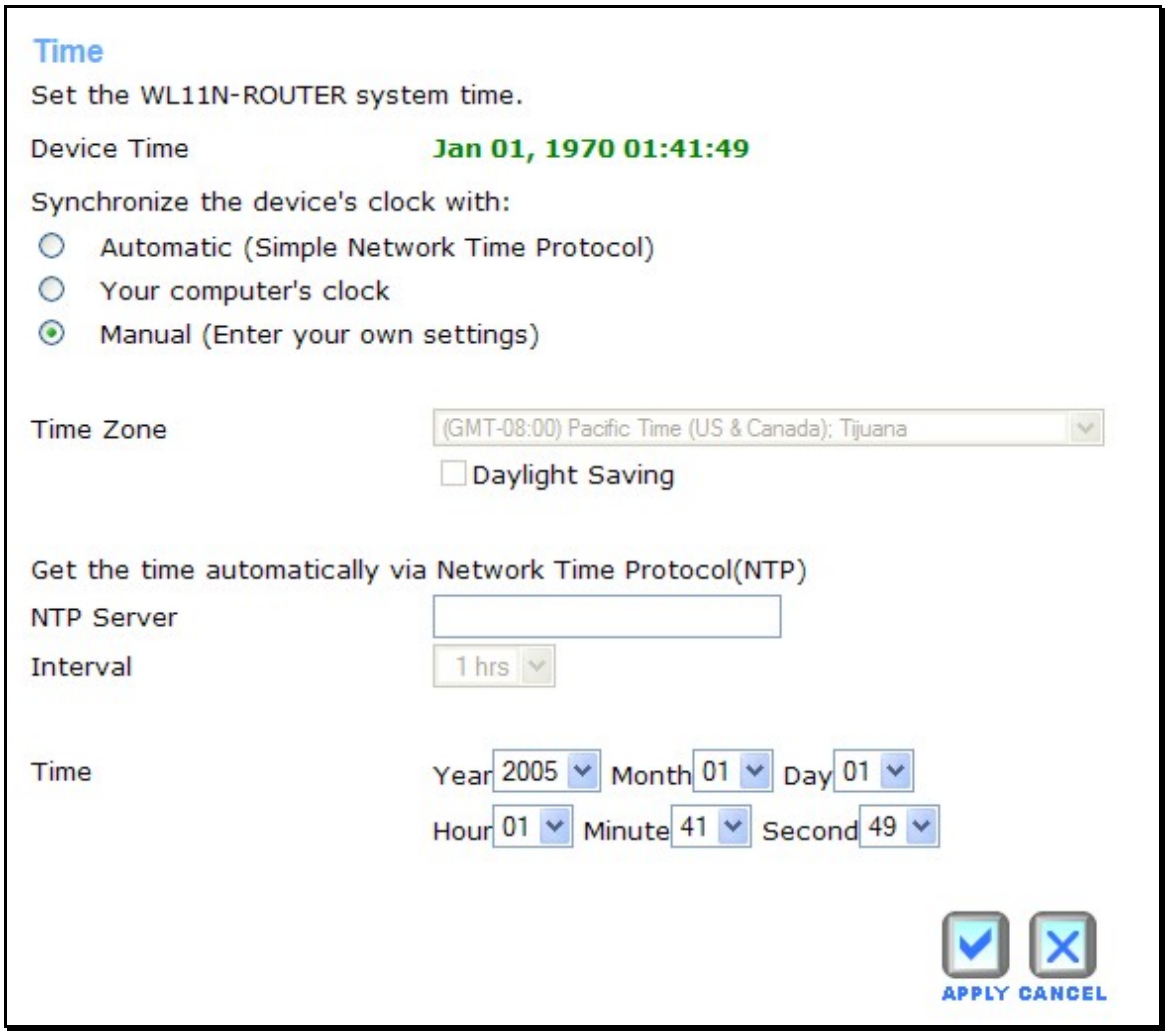
Under the Administrator heading, type the **New Password** and **Confirm Password** to be certain you have typed it correctly. Click the **Apply** button to activate the new password. The System User Name remains “admin”, this cannot be changed using the web manager interface. Be sure to save the new setting.

Remote Web Access

The **Administrator Settings** window is also used to enable remote management access to the router. To enable remote management of the router, select the Enabled radio button and type the IP Address of the remote network used for management. Click the **Apply** button to activate remote management from the chosen IP address.

Time

The router provides a number of options to maintain current date and time including SNTP.



Time settings menu

To configure system time on the router, select the method used to maintain time. The options available include SNTP, using your computer's system clock or set the time and date manually. If you opt to use SNTP, you must enter the SNTP server URL or IP address. Click the **Apply** button to set the system time.

System

Once you have configured the router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **System** button in the **Tools** directory to display the **System Management** menu. Click the **Save** button to Save Settings to Local Hard Drive. You will be prompted to select a location on your computer to put the file. The file type is .xml (HTML) and may be named anything you wish.

System Settings menu

Save or Load Configuration File

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Restore** button to Load Settings From Local Hard Drive. Confirm that you want to load the file when prompted and the process is completed automatically. The router will reboot and begin operating with the configuration settings that have just been loaded.

Reset to Factory Default Settings

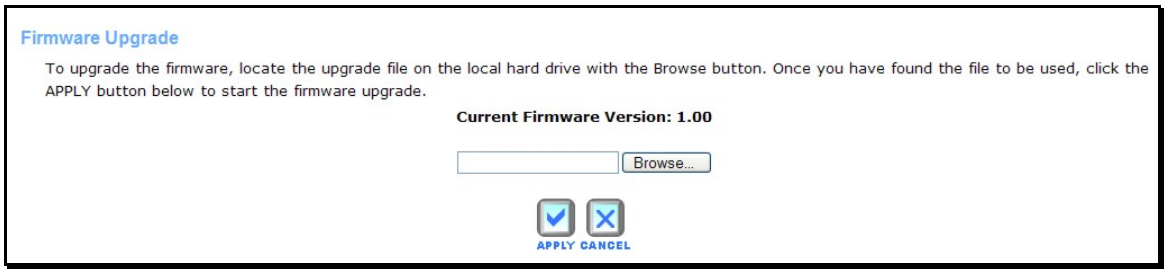
To reset the router to its factory default settings, click the **Reset** button. You will be prompted to confirm your decision to reset the router. The router will reboot with the factory default settings including IP settings (192.168.1.1) and Administrator password (admin).

To simply restart the router, click the **Reboot** button.

Firmware

Use the **Firmware Upload** menu to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the **System Settings** menu described above.

NOTE: Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the router's configuration settings before upgrading the firmware.

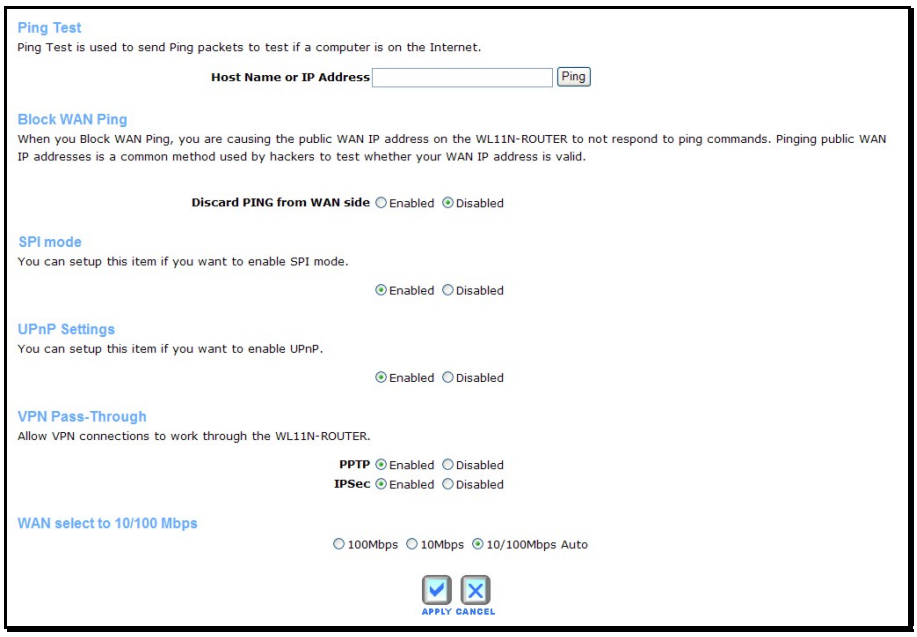


Firmware Upgrade

To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the file. Click the **Apply** button to begin copying the file. The file will load and restart the router automatically. Do not turn off the power while the router is upgrading the firmware.

Miscellaneous

To perform a statndard Ping test for network connectivity, click the **Misc.** window button in the **Tools** directory to view the **Miscellaneous Configuration** window.



Miscellaneous Configuration menu

Ping Test

The Ping test functions on the WAN and LAN interfaces. Type the **Host Name or IPAddress** you want to check in the space provided and click the **Ping** button. Read the Ping test result in the space immediately below

Block WAN Ping

The Block WAN Ping feature allows the user to block hackers who may be trying to test whether your WAN IP address is valid.

SPI mode

Stateful Packet Inspection mode is an active firewall the user can enable to keep track of the state of network connections.

UPnP Settings

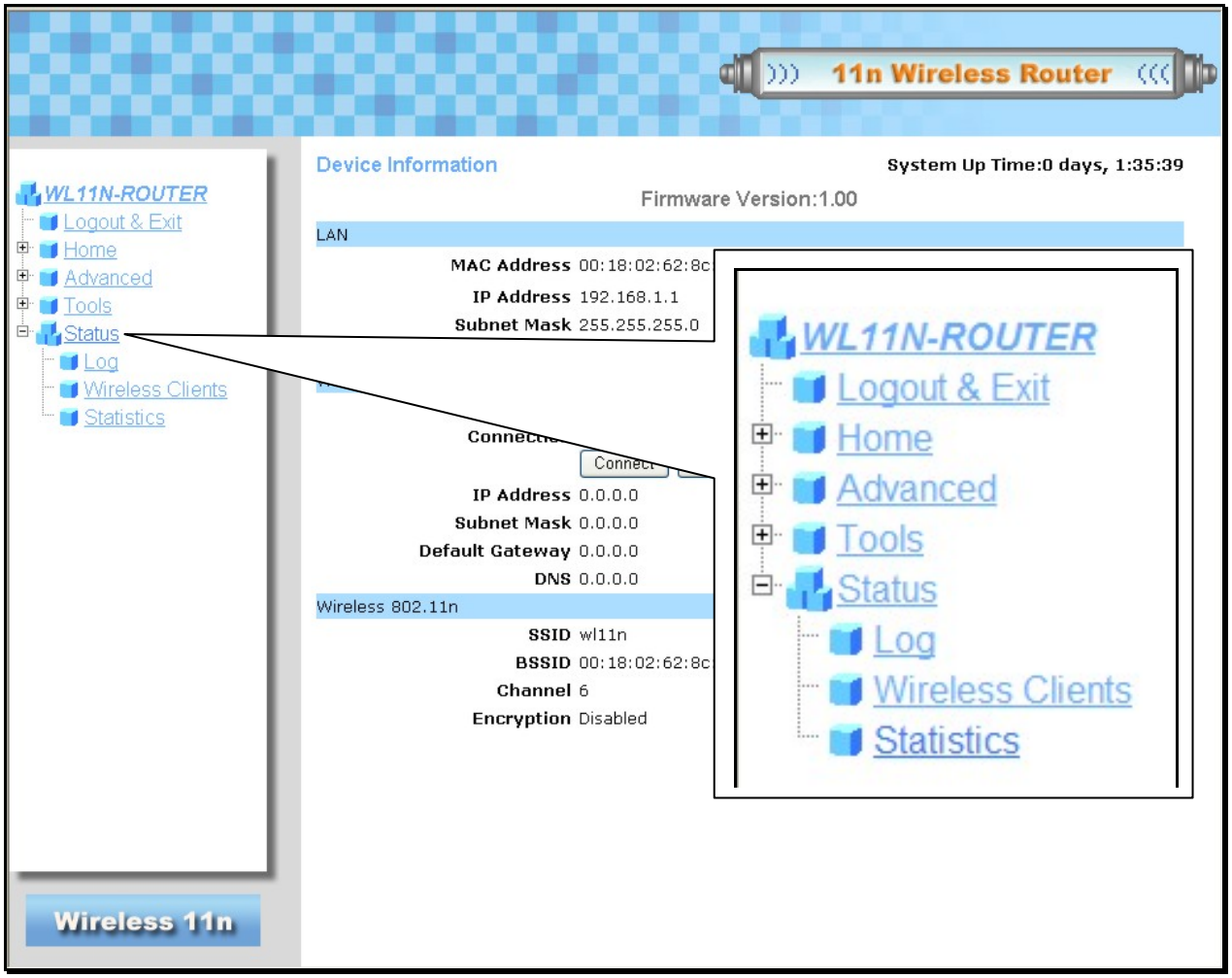
UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network. UPnP is a protocol supported by diverse networking media including Ethernet, Firewire, phone line, and power line networking.

VPN Pass-Through

This feature allows VPN connections to pass through the router. It is enabled by default.

Status

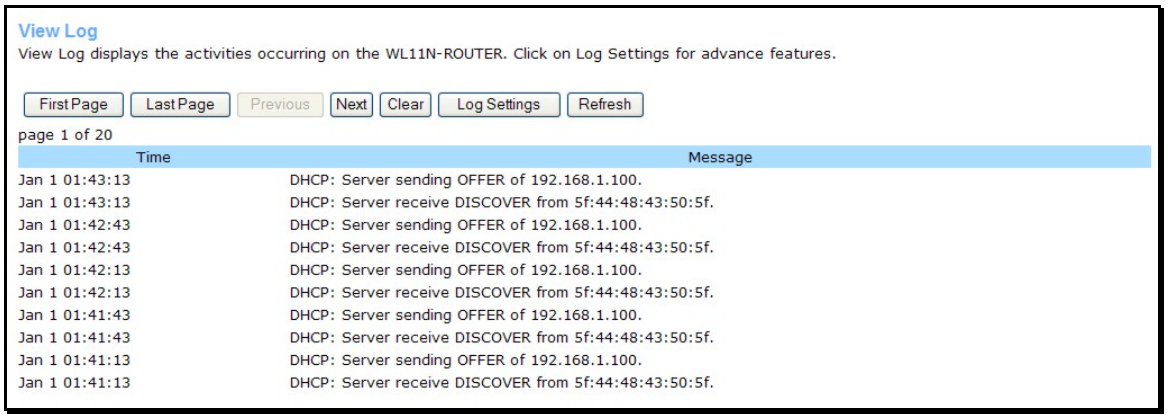
Use these display menus to view system information and monitor performance. Click the **Status** directory link to reveal the menu links for various functions located in this directory. The **Device Information** display is the first item in the **Status** directory.



Status Directory menus

Log

The system log displays chronological event log data. Use the navigation buttons to view or scroll log pages.

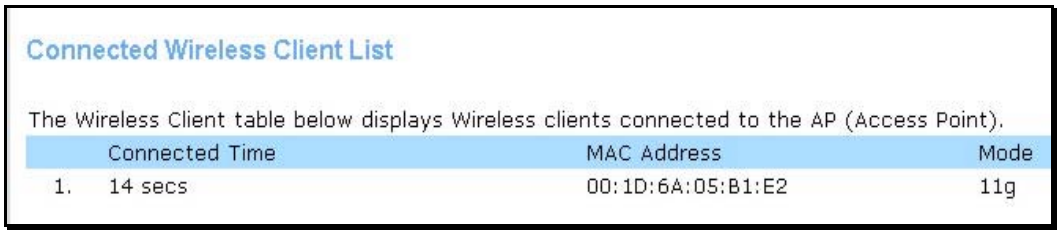


View Log menu

Use the Set Log Options menu arrange for email alerts from the log.

Wireless Clients

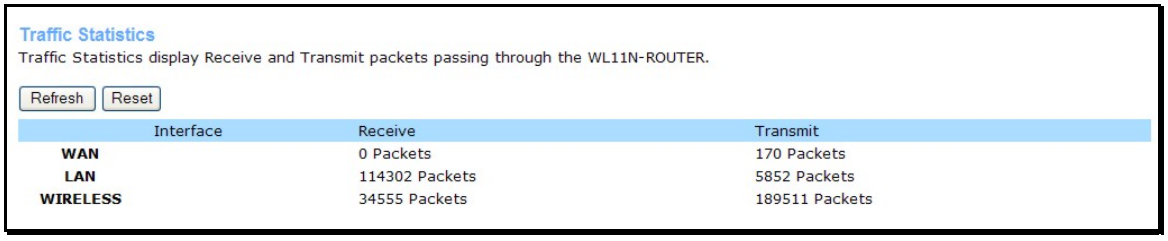
This window displays all the wireless clients currently connected to the acess point.



Wireless Client List display menu

Statistics

Use this window to monitor traffic on the WAN, LAN, and Wireless connections.



Traffic Statistics

Click **Refresh** to view updated traffic information. Click **Reset** to return packets counts to zero.

Technical Specifications

Power Adapter:	Output: 5V DC, 2.5~3A
Standards:	IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.3 IEEE 802.3u
Management	Web-based
LED	WPS Blinks blue for 120 seconds while searching for WPS enabled station. LAN Steady green light for valid link, blinks when for activity. WLAN Steady green light for valid link, blinks when for activity. WAN Steady green light for valid link, blinks when for activity. Status Blinks green when system function is normal. Power Steady green when powered on.
Operating Temperature	0ºC to 40ºC (32ºF to 104ºF)
Humidity	10% to 95% non-condensing
Dimensions	200 mm x 120 mm x 34 mm
Weight	320 gm
Certifications	EMI: FCC Class B, CE Class B

Modulation	IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK IEEE 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM IEEE 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM
Frequency	2400 ~ 2484.5MHz ISM band
Channels	11 channels for United States 13 channels for European Countries 13 channels for Japan
Operating Range	Indoors – up to 328 feet (100 meters) Outdoors – up to 1312 feet (400 meters)
Transmit Power	11g: 14dBm Typical 11b: 17dBm Typical
Media Access Protocol	CSMA/CA with ACK
WEP	64/128 bits
Wireless Certification	Wi-Fi WPA
Antenna type	2.0 dbi external dipole

Configuring IP Settings on Your Computer

In order to configure your system to receive IP settings from the router it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. Below is an illustrated example of how to configure a Windows XP system to automatically obtain IP settings from the router. Following this example is a step-by-step description of the procedures used on the other Windows operating systems to first check if the TCP/IP protocol has been installed; if it is not, instructions are provided for installing it. Once the protocol has been installed you can configure the system to receive IP settings from the router.

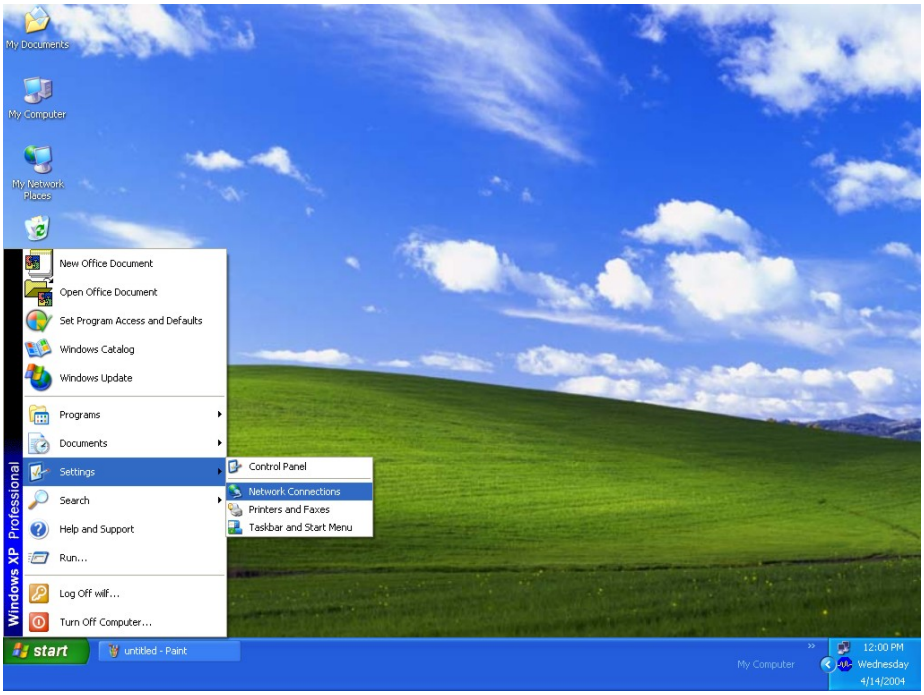
For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP address from the router, that is, configure the system to be a DHCP client.

NOTE: If you are using this router to provide Internet access for more than one computer, you can use these instructions later to change the IP settings for the other computers. However, you cannot use the same IP address since every computer must have its own IP address that is unique on the local network.

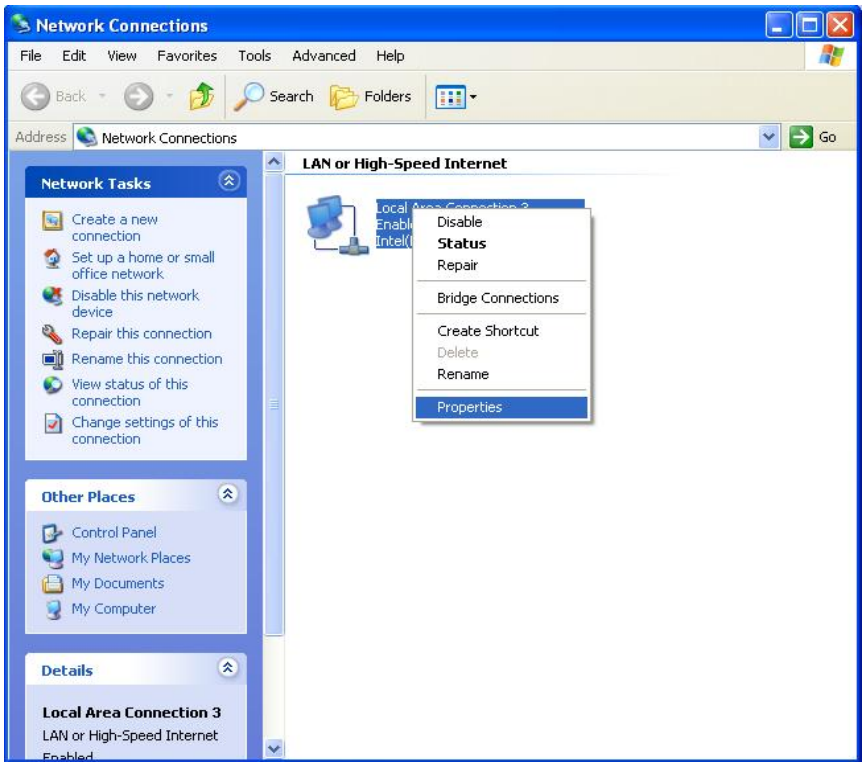
Configure Windows XP for DHCP

Use the following steps to configure a computer running Windows XP to be a DHCP client.

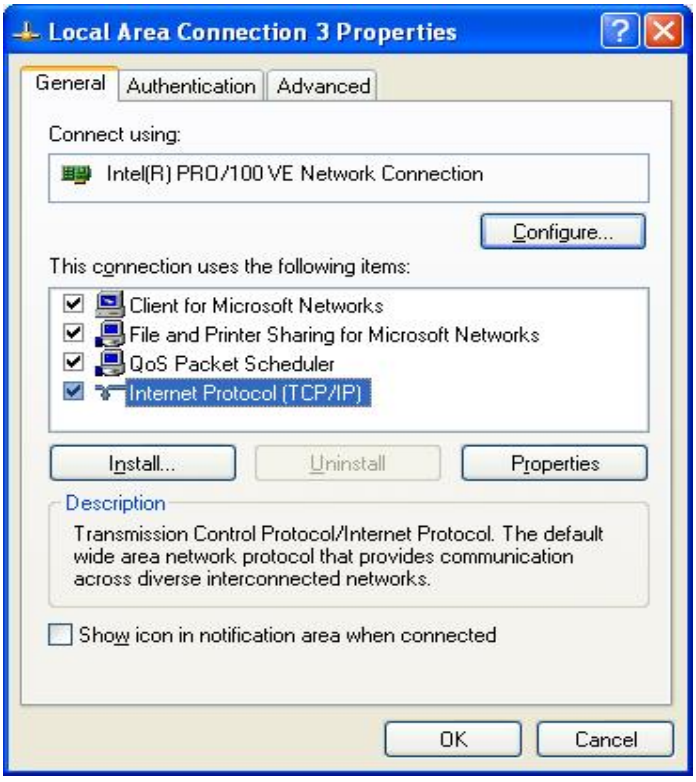
1. From the **Start** menu on your desktop, go to **Settings**, then click on **Network Connections**.



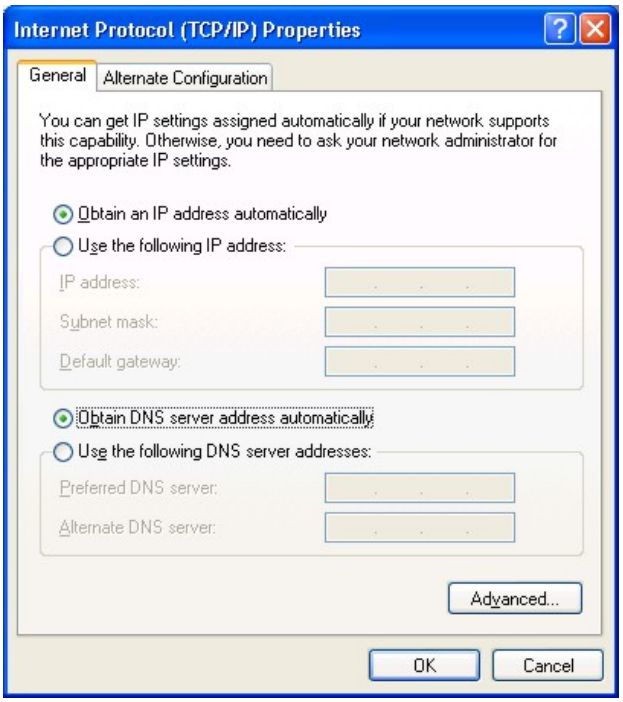
2. In the **Network Connections** window, right-click on **LAN** (Local Area Connection), then click **Properties**.



3. In the **General** tab of the **Local Area Connection Properties** menu, highlight **Internet Protocol (TCP/IP)** under "This connection uses the following items:" by clicking on it once. Click on the **Properties** button.



4. Select "Obtain an IP address automatically" by clicking once in the circle. Click the **OK** button.



Your computer is now ready to use the router's DHCP server.

Windows 2000

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
4. The **Local Area Connection Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, skip ahead to *Configure Windows 2000 for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Install**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
8. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
9. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows 2000 for DHCP

1. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
2. In **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
3. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the button labeled **Obtain an IP address automatically**.
5. Double-click **OK** to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the router's DHCP server.

Windows 95 and Windows 98

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**. Double-click the **Network** icon.
2. The **Network** dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled, skip to *Configure IP Information Windows 95, 98*.
3. If TCP/IP does not display as an installed component, click **Add**. The **Select Network Component Type** dialog box displays.
4. Select **Protocol**, and then click **Add**. The **Select Network Protocol** dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click **OK** to return to the Network dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click **OK** to restart the PC and complete the TCP/IP installation.

Configure Windows 95 and Windows 98 for DHCP

1. Open the **Control Panel** window, and then click the **Network** icon.
2. Select the network component labeled TCP/IP, and then click **Properties**.
3. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
4. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
5. Click the **Obtain an IP address automatically** option.
6. Double-click **OK** to confirm and save your changes. You will be prompted to restart Windows.
7. Click **Yes**.

When it has restarted, your computer is ready to use the router's DHCP server.

Windows ME

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Star**t button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
4. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip ahead to *Configure Windows ME for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Microsoft** in the Manufacturers box.

8. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
9. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
10. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows ME for DHCP

1. In the **Control Panel**, double-click the **Network and Dial-up Connections** icon.
2. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
3. In the **Network Properties** dialog box, select **TCP/IP**, and then click **Properties**.
4. In the **TCP/IP Settings** dialog box, click the **Obtain and IP address automatically** option.
5. Double-click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the router's DHCP server.

Windows NT 4.0 Workstations

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows NT** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. In the **Control Panel** window, double-click the **Network** icon.
3. In the **Network** dialog box, click the **Protocols** tab.
4. The **Protocols** tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to "Configure IP Information"
5. If TCP/IP does not display as an installed component, click **Add**.
6. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click **OK**. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
7. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
8. Click **Yes** to continue, and then click **OK** if prompted to restart your computer.

Configure Windows NT 4.0 for DHCP

1. Open the **Control Panel** window, and then double-click the **Network** icon.
2. In the **Network** dialog box, click the **Protocols** tab.
3. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
4. In the **Microsoft TCP/IP Properties** dialog box, click the **Obtain an IP address automatically** option.
5. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the router's DHCP server.

FCC Warning statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
3. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user’s authority to operate the equipment.